UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

JANE DOE, *individually, and on behalf of all others similarly situated,* Plaintiff, v. WELLSTAR HEALTH SYSTEM, INC., Defendant.	Case No. **COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Jane Doe ("Plaintiff"),[1] a patient of Wellstar Health System, Inc. ("Wellstar" or "Defendant"), brings this class action lawsuit against Wellstar individually and on behalf of all others similarly situated and alleges, upon personal

[1] In order to avoid compounding the injuries and damages which give rise to this putative class action lawsuit and given the highly sensitive nature of the non-public, confidential and highly sensitive personal health information disclosed by Defendant without consent, Plaintiff will move this Honorable Court for permission to proceed anonymously. *See, e.g.*, *Doe v. Archdiocese of Atlanta*, 328 Ga. App. 324, n. 20, 761 S.E.2d 864, 869 (2014).

knowledge as to her own actions and her counsel's investigation and upon information and good faith belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this action individually and on behalf of millions of other patients (collectively, the "Users") whose medical privacy was violated by Wellstar's use of Meta Platforms, Inc., d/b/a Meta's ("Meta" or "Facebook") tracking and collection tools.[2]

2. Plaintiff, a Wellstar patient, alleges that Wellstar installed Meta Collection Tools on its public website (https://www.wellstar.org/, the "Website") and its "Wellstar MyChart" patient portal (available at mychart.wellstar.org, "MyChart" or the "Patient Portal") (collectively, the "Web Properties") to share her confidential health information ("Private Information," including personally identifiable information ("PII") and protected health information ("PHI")) with Meta in violation of federal and state laws.

3. Wellstar used Meta Collection Tools to divulge the Private Information of Users of its Web Properties for marketing, re-marketing and analytics purposes

[2] The Facebook tracking and collection tools include the Meta Pixel, Meta SDK, Meta Conversions API, customer list uploads, social plug-ins, the Meta Graph API, server-to-server transmissions and similar collection tools (collectively, "Meta Collection Tools").

despite its express promise that: "Wellstar may only use and disclose PHI as permitted by law or with the written authorization of the patient or the patient's representative."[3]

4. The Private Information of potentially millions of active or potential patients of Wellstar's Web Properties was improperly and unlawfully disclosed to Facebook without their knowledge or consent. Wellstar did so because it knew that this sensitive information had tremendous value and that Plaintiff and Class Members would ***not*** consent to the collection, disclosure and use of their Private Information if they were provided a choice or would demand significant compensation.

5. Wellstar encouraged and/or required Plaintiff and Class Members to use its Web Properties, including MyChart, to receive healthcare services, and Defendant's Web Properties encourage and require Users to provide Private Information in order to facilitate healthcare treatment including, but not limited to, to search for a doctor, learn more about their conditions and treatments, access medical records and test results and manage appointments.

---

[3] *See* https://www.wellstar.org/financial-policy-and-privacy-info/internet-privacy-policy (last visited Apr. 12, 2024).

6. At all times that Plaintiff and Class Members visited and utilized Defendant's Website and MyChart portal to receive medical services, they had a reasonable expectation of privacy that their Private Information would remain secure and protected and only utilized for medical purposes.

7. Further, Wellstar made express and implied promises to protect Plaintiff's and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchange with Defendant.

8. Simply put, Wellstar broke those promises again and again.

9. The Facebook tracking pixel (the "Meta Pixel"), installed and configured by Defendant Wellstar, is a "piece of code" that allowed Defendant to "measure the effectiveness of [its] advertising by understanding the actions [Users] take on [its] site."[4] It also allowed Defendant to optimize the delivery of ads, measure cross-device conversions, create custom advertising groups or "audiences," learn about the use of the Web Properties, and optimize advertising and marketing costs.[5]

[4] https://www.facebook.com/business/help/742478679120153?id=2053766828321 42 (last visited Apr. 19, 2024).

[5] *Id.*

10. Invisible to the naked eye, pixels—which are configured by the website owner, here, Wellstar—collect and transmit information from Users' browsers to unauthorized third parties including, but not limited to, Meta/Facebook.[6]

11. In particular, the Meta Pixel tracks visitors to the Web Properties and the actions they take as they interact with the website, including how long a person spends on a particular web page, which buttons the person clicks, which pages they view and the text or phrases they type into various portions of the website (such as a general search bar, chat feature or text box). [7]

12. Wellstar intentionally installed the Meta Pixel on its Web Properties and configured the Meta Pixel to transmit and disclose Plaintiff's and Class Members' Private Information to Facebook.

---

[6] The Meta Pixel itself is a small snippet of code placed on webpages by the website owner. The process of adding the Meta Pixel to a webpage is a multi-step process that must be undertaken by the website owner, namely, Wellstar.

[7] A pixel is a piece of code that "tracks the people and type of actions they take." RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Apr. 19, 2024). Pixels are routinely used to target specific customers by utilizing the data gathered through the pixel to build profiles for the purposes of retargeting and future marketing. Upon information and belief, Defendant utilized the Meta Pixel data to improve and save costs on its marketing campaign, improve its data analytics, and attract new patients.

13. Operating as designed, Defendant's Meta Pixel allowed the Private Information that Plaintiff and Class Members submitted to Wellstar to be unlawfully disclosed to Facebook.

14. For example, when a User uses Wellstar's Web Properties, the Meta Pixel directed Plaintiff's or Class Members' browser to send a message to Facebook's servers, those messages transmitted the content of their communications to Meta, including, but not limited to: (1) signing-up for the Patient Portal; (2) signing-in or -out of the Patient Portal; (3) taking actions inside the Patient Portal; (4) making, scheduling, or participating in appointments; (5) exchanging communications relating to doctors, treatments, payment information, health insurance information, prescription drugs, prescription side effects, conditions, diagnoses, prognoses, or symptoms of health conditions; (6) conduct a search on Wellstar's Web Properties and (7) other information that qualifies as PHI under federal and state laws.

15. The information transmitted from Wellstar's Web Properties to Meta includes information sufficient to identify a specific patient under federal law (such as IP address information, device identifiers, and advertising identifiers that Meta associates with a patient's Facebook account), and may also include a patient's demographic information, email address, phone number, computer ID address or contact information entered as emergency contacts or for advanced care planning,

along with information like appointment type and date, a selected physician, button and menu selections, the content of buttons clicked and typed into text boxes, and information about the substance, purport, and meaning of patient requests for information from Wellstar under federal and state health privacy laws.

16. Among the personally identifying information that Defendant discloses is the User's unique and persistent Facebook ID which allows Facebook and other third parties to personally identify that User and associates the Users' Private Information with its Facebook profile. The Facebook ID is a string of numbers Facebook uses to identify and connect to a User's Facebook profile. Facebook creates a Facebook ID automatically, whether or not you choose to create a username.[8] Thus Facebook, which creates and maintains the Facebook ID directly connected to a User's Facebook account, utilizes the Facebook ID to personally identify each User whose Private Information is disclosed to it.

17. Transmitting the Private Information allows a third party (*e.g.*, Meta/Facebook) to know that a specific patient was seeking confidential medical care. This type of disclosure could also allow a third party to reasonably infer that a

[8] *See* https://www.facebook.com/help/211813265517027 (last visited Apr. 19, 2024).

specific patient was being treated for a specific type of medical condition such as cancer, pregnancy or AIDS.

18. Meta collects the transmitted identifiable health information and uses "cookies" to match it to Facebook users allowing Wellstar to target advertisements both on and off Facebook. For example, Wellstar and Meta can target ads to a person who has used the Website or the Patient Portal and exchanged communications about a specific condition, such as cancer.

19. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (1996) and Georgia law relating to the confidentiality of medical records, O.C.G.A. §§ 31-33-2, 31-33-8, both prohibit healthcare providers from sharing health care information, medical records and related information with third parties except as needed for a patient's treatment, payment or with their consent. Importantly, these laws give patients a reasonable expectation of privacy in communications with healthcare providers relating to their medical conditions and treatment, because this information may not be disclosed outside the healthcare setting without notice and consent.

20. The Office for Civil Rights ("OCR") at the United States Department of Health and Human Services ("HHS") recently affirmed that HIPAA and its regulations prohibit the transmittal of individually identifiable health information ("IIHI") by tracking technology like the Meta Pixel without the patient's

authorization and other protections like a business associate agreement with the recipient of patient data.[9]

21. Reiterating the importance of and necessity for data security and privacy concerning health information, the Federal Trade Commission ("FTC") recently published a bulletin entitled *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases*, in which it noted that:

> [h]ealth information is not just about medications, procedures, and diagnoses. ***Rather, it is anything that conveys information—or enables an inference—about a consumer's health***. Indeed, [recent FTC enforcement actions involving] *Premom*, *BetterHelp*, *GoodRx* and *Flo Health* ***make clear that the fact that a consumer is using a particular health-related app or website—one related to mental health or fertility, for example—or how they interact with that app (say, turning 'pregnancy mode' on or off) may itself be health information.***[10]

---

[9] *See* Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html* (noting that "IIHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as in some circumstances IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.").

[10] *See* Elisa Jillison, *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases*, the FTC Business Blog (July 25, 2023) (emphasis added), available at https://www.ftc.gov/business-

22. The FTC is unequivocal in its stance as it informs—in no uncertain terms—healthcare companies that they should ***not*** use tracking technologies to collect sensitive health information and disclose it to various platforms without informed consent:

> **Don't use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers.**
>
> In today's surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. ***But when companies use consumers' sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out.***
>
> [Recent FTC enforcement actions such as] *BetterHelp*, *GoodRx*, *Premom*, and *Flo* make clear that practices like that ***may run afoul of the FTC Act if they violate privacy promises or if the company fails to get consumers' affirmative express consent for the disclosure of sensitive health information***.[11]

23. Not only did Wellstar willfully and intentionally incorporate the tracking Meta Pixel into its Web Properties, but it also never disclosed to Plaintiff

---

guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases (last visited Apr. 19, 2024).

[11] *Id.* (emphasis added) (further noting that *GoodRx* & *Premom* underscore that this conduct may also violate the Health Breach Notification Rule, which requires notification to consumers, the FTC and, in some cases, the media, of disclosures of health information without consumers' authorization.

or Class Members that it shared their sensitive and confidential communications via the Web Properties with Facebook.

24. As a result, Plaintiff and Class Members were unaware that their PII and/or PHI were being surreptitiously transmitted to Facebook as they communicated with their healthcare providers, looked up their conditions and/or treatments, and logged into the MyChart portal.[12]

25. The full extent of Wellstar's unlawful disclosures is not yet known, but the numbers may be staggering. According to Wellstar's Website, "Wellstar [is] one of Georgia's largest and most integrated nonprofit health systems with **more than**

[12] In contrast to Defendant, several healthcare providers which have installed the Meta Pixel on their Web Properties have provided their patients with notices of data breaches caused by the Pixel transmitting PHI to third parties. *See*, *e.g.*, *Cerebral, Inc. Notice of HIPAA Privacy Breach*, https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf (last visited Apr. 19, 2024); Annie Burky, *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies*, FIERCE HEALTHCARE (October 20, 2022), https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3 (last visited Apr. 19, 2024); *Novant Health Notifies 1.3M Patients of Unauthorized PHI Disclosure Caused By Meta Pixel* (August 17, 2022), https://healthitsecurity.com/news/novant-health-notifies-patients-of-unauthorized-phi-disclosure-caused-by-meta-pixel#:~:text=August%2017%2C%202022%20%2D%20North%20Carolina,protected%20health%20information%20(PHI) (last visited Apr. 19, 2024).

300 locations, including 11 hospitals and 25,000 team members."[13] For its fiscal year ending in June 2023, its net income was over $370 million.

26. Defendant owed common law, contractual, statutory, and regulatory duties to keep Plaintiff's and Class Members' communications and medical information safe, secure and confidential. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized disclosure.

27. Wellstar, however, failed in its obligations and promises by utilizing Meta Collection Tools on its Web Properties, particularly the Meta Pixel, knowing that such technology would transmit and share Plaintiff's and Class Members' Private Information with unauthorized third parties. Defendant breached its obligations in one or more of the following ways: (i) failing to adequately review its marketing programs and web-based technology to ensure their Web Properties were safe and secure; (ii) failing to remove or disengage technology that was known and designed to share Users' information; (iii) failing to obtain the consent of Plaintiff and Class Members to disclose their Private Information to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiff's and Class Members'

[13] https://careers.wellstar.org/about-us (emphasis added) (last visited Apr. 12, 2024).

Private Information through the Meta Pixel or any other tracking technologies; (v) failing to warn Plaintiff and Class Members; and (vi) otherwise failing to design, and monitor its Web Properties in order to maintain the confidentiality and integrity of patient Private Information.

28. Wellstar's interception, dissemination, and use of Private Information not only violates federal and state law but also harms patients by intruding upon their privacy; erodes the confidential nature of the provider-patient relationship; takes patients' property and property rights without compensation and ignores their right to control the dissemination of their health information to third parties.[14]

29. Wellstar has also been unjustly enriched by its misconduct, obtaining unearned revenues derived from the enhanced advertising services and more cost-efficient marketing on Facebook it receives in exchange for its unauthorized disclosure of patient information.

30. Plaintiff seeks to remedy these harms individually and for millions of similarly affected persons, and therefore brings causes of action for (1) Invasion of Privacy; (2) Breach of Fiduciary Duty; (3) Negligence; (4) Negligence Per Se; (5)

[14] It is unknown without discovery whether the Private Information was further disseminated to additional third-party marketing companies (*e.g.*, Google, Twitter, Bing, LinkedIn, HotJar, LifePerson, The Trade Desk or Adobe) for the purposes of building profiles and retargeting or to insurance companies to set rates.

Breach of Implied Contract; (6) Breach of Contract; (7) Unjust Enrichment; and (8) Violations of the Electronic Communications Privacy Act, 18 U.S.C. § 2511(1), *et seq.*

PARTIES

31. Plaintiff Jane Doe is a natural person, citizen of Georgia and a resident of Cobb County.

32. Defendant Wellstar Healthcare, Inc. is a Georgia company with its principal place of business at 793 Sawyer Road, Marietta, GA 30062. Defendant is a Georgia-wide integrated network of physician clinics, outpatient centers and hospitals. Its network consists of 11 hospitals, 10 emergency departments, 329+ medical offices, 90+ rehabilitation centers, served by approximately 25,000 employees.[15]

33. Headquartered in Marietta, Wellstar is one of the largest health systems in the state of Georgia. Defendant advertises that it is committed to "enhance the health and wellbeing of every person we serve," and serves millions of patients annually.[16]

34. Defendant is a covered entity under HIPAA.

---

[15] *See* https://www.wellstar.org/about-us (last visited Apr. 12, 2024)

[16] *Id.*

JURISDICTION & VENUE

35. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 over the claims that arise under federal law, including the Electronic Communications Privacy Act ("ECPA"), 28 U.S.C. § 2511, *et seq.*

36. The Court has supplemental jurisdiction over Plaintiff's claims arising under state law under 28 U.S.C. § 1367.

37. This Court also has subject matter jurisdiction under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than one hundred members in the proposed Class, and at least one member of the class is a citizen of a state different from Defendant.

38. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and a substantial portion of the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

39. Venue is proper under 28 U.S.C. § 1391(b)(1) and (2) because Defendant resides in this district and a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this district.

FACTUAL BACKGROUND

I. WELLSTAR SECRETLY DISCLOSED & PERMITTED THIRD PARTIES TO INTERCEPT PLAINTIFF'S & CLASS MEMBERS' PHI.

40. Wellstar maintains and operates the Web Properties, by and through which Wellstar encouraged and/or required patients to seek healthcare services.

41. To obtain healthcare services through the Web Properties, Plaintiff and other Class Members were required to provide their PHI and/or PII to Wellstar.

42. Each step of this process was tracked and logged by the Meta Pixel.

43. On information and good faith belief, throughout the Class Period, the process for obtaining healthcare services on the Web Properties has been substantially the same in all material respects throughout the United States.

44. Completely unbeknownst to Plaintiff and other Class Members, beginning in approximately June 2016 and continuing to at least June 2022, Private Information that they communicated to Wellstar through the Website while obtaining healthcare services was disclosed to Meta.

A. Wellstar Improperly Disclosed Plaintiff's & Class Members' Private Information.

45. Wellstar utilized Facebook advertisements and intentionally installed the Meta Pixel on its Web Properties.

46. Meta's Health division is dedicated to marketing to and servicing Meta's healthcare Partners. Meta defines its Partners to include businesses that use

Meta's products, including the Meta Pixel or Meta Audience Network tools to advertise, market, or support their products and services.

47. Meta works with hundreds of Meta healthcare Partners, using Meta Collection Tools to learn about visitors to their websites and leverage that information to sell targeted advertising based on patients' online behavior. Meta's healthcare Partners also use Meta's other ad targeting tools, including tools that involve uploading patient lists to Meta.[17]

48. Meta offers an ad targeting option called "Custom Audiences." When a patient takes an action on a Meta healthcare Partner's website embedded with the Meta Pixel, the Meta Pixel will be triggered to send Meta "Event" data that Meta matches to its Users. A web developer can then create a "Custom Audience" based on Events to target ads to those patients. The Meta Pixel can then be used to measure the effectiveness of an advertising campaign.[18]

---

[17] Meta Business Help Center, *About Customer List Custom Audiences* (2023), *https://www.facebook.com/business/help/341425252616329?id=2469097953376494*.

[18] Meta Business Help Center, *About Customer List Custom Audiences* (2023), *https://www.facebook.com/business/help/341425252616329?id=2469097953376494*; *see also,* Meta Blueprint, Connect your data with the Meta Pixel and Conversion API (2023), *https://www.facebookblueprint.com/student/activity/212738?fbclid=IwAR3HPO1d_fnzRCUAhKGYsLqNA-VcLTMr3G_hxxFr3GZC_uFUcymuZopeNVw#/page/5fc6e67d4a46d349e9dff7fa*

49. Meta also allows Meta healthcare Partners to create a Custom Audience by uploading a patient list to Meta. As Meta describes it:[19]

> A Custom Audience made from a customer list is a type of audience you can create to connect with people who have already shown an interest in your business or product. It's made of information - called "identifiers" - you've collected about your customers (such as email, phone number and address) and provided to Meta. Prior to use, Meta hashes this information.
>
> Then, we use a process called matching to match the hashed information with Meta technologies profiles so that you can advertise to your customers on Facebook, Instagram and Meta Audience Network. The more information you can provide, the better the match rate (which means our ability to make the matches). Meta doesn't learn any new identifying information about your customers.

50. Meta provides detailed instructions for healthcare Partners to send their patients' individually identifiable information to Meta through the customer list upload. For example:

[19] Meta Business Help Center, *About Customer List Custom Audiences* (2023), *https://www.facebook.com/business/help/341425252616329?id=246909795337649 4*.

> **Prepare your customer list in advance.** To make a Custom Audience from a customer list, you provide us with information about your existing customers and we match this information with Meta profiles. The information on a customer list is known as an "identifier" (such as email, phone number, address) and we use it to help you find the audiences you want your ads to reach.
>
> Your customer list can either be a CSV or TXT file that includes these identifiers. To get the best match rates, use as many identifiers as possible while following our formatting guidelines. You can hover over the identifiers to display the formatting rules and the correct column header. For example, **first name** would appear as **fn** as a column header in your list.
>
> Alternatively, we have a file template you can download to help our system map to your identifiers more easily. (You can upload from Mailchimp as well.)

51. Meta healthcare Partners can then use the Custom Audiences derived from their patient list with the Meta Pixel and Pixel Events for Meta marketing campaigns and to measure the success of those campaigns.

52. Without discovery, Plaintiff does not yet know whether Wellstar uploaded patient lists to Meta. However, Plaintiff does know that when they and Class Members sought and used Defendant's Web Properties, their Private Information was intercepted concurrently in real time and then disseminated to Facebook and potentially to other third parties, via the Meta Pixel and other Meta Collection Tools that Defendant secretly installed on its Web Properties.

53. Plaintiff and Class Members did not intend or have any reason to suspect their Private Information would be shared with Facebook or that Defendant was tracking their every movement and disclosing same to Facebook when they entered highly sensitive information on Defendant's Web Properties.

54. Defendant did not disclose to or warn Plaintiff or Class Members that Defendant used Plaintiff's and Class Members' Web Properties submissions for Facebook's marketing purposes.

55. Defendant installed the Meta Pixel used to disclose Plaintiff's and Class Members' Private Information via the Meta Pixel from at least June 2016.

56. Plaintiff and Class Members never consented, agreed, authorized or otherwise permitted Defendant to disclose their Private Information to Meta.

57. Defendant's unauthorized disclosure is not just limited to activity on the public Website, but the disclosure also involved information contained within the highly sensitive and private MyChart Portal, which requires patients to enter a specific login.

58. Wellstar disclosed to Meta the following non-public private information:

a. when a patient clicks to register for the Patient Portal;

b. information that a patient types into registration forms including their name, email address, and zip code;

c. when a patient clicks to log in to the Patient Portal;

d. when a patient sets up or schedules an appointment;

e. information that a patient types into or chooses on an appointment form;

f. when a patient clicks a button to call the provider from a mobile device directly from the Website;

g. descriptive URLs that describe the categories of the Website, categories that describe the current section of the Website, and the referrer URL that caused navigation to the current page;

h. the communications a patient exchanges through Wellstar's Web Properties by clicking and viewing webpages, including communications about providers and specialists, conditions, and treatments, along with the timing of those communications, including whether they are made while a patient is still logged in to the Patient Portal or around the same time that the patient has scheduled an appointment, called the medical provider, or logged into the Patient Portal; and

i. the same or substantially similar communications that patients exchange with health insurance companies, pharmacies, and prescription drug companies.

59. Defendant deprived Plaintiff and Class Members of their privacy rights when it: (1) implemented technology (i.e. Meta Pixels) that surreptitiously tracked, recorded and disclosed Plaintiff's and other Users' confidential communications and Private Information; (2) disclosed patients' protected information to Meta—an unauthorized third party and (3) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

B. Meta's Collection Tools Redirect Patients' Data from Wellstar's Web Properties to Facebook to Use for Ad Targeting.

60. Facebook operates the world's largest social media company and generated nearly $117 billion in revenue in 2022, roughly 97% of which came from selling targeted advertising. [20]

61. As a core part of its business, Facebook maintains profiles on users that include the user's real names, locations, email addresses, friends, likes and communications that Facebook associates with personal identifiers, including IP addresses, cookies, device identifiers and advertising ID identifiers.

62. Facebook also tracks non-Facebook users through its widespread internet marketing products and source code, such as the Meta Pixel.

63. Facebook then sells advertising space by highlighting its ability to target users.[21] Facebook can target users so effectively because it surveils user activity both on and off its site.[22] This allows Facebook to make inferences about

---

[20] FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2022 RESULTS, https://investor.fb.com/investor-news/press-release-details/2023/Meta-Reports-Fourth-Quarter-and-Full-Year-2022-Results/default.aspx (last visited Jan. 12, 2024).

[21] WHY ADVERTISE ON FACEBOOK, https://www.facebook.com/business/help/205029060038706 (last visited Jan. 12, 2024).

[22] ABOUT FACEBOOK PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Jan. 12, 2024).

users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[23]

64. Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[24]

65. Indeed, Facebook utilizes the precise type of information disclosed by Defendant to identify, target, and market products and services to individuals.

66. Advertisers can also build "Custom Audiences."[25] Custom Audiences enable advertisers to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[26]

67. With Custom Audiences, advertisers can target existing customers directly, and they can also build "Lookalike Audiences," which "leverages

---

[23] AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting (last visited Jan. 12, 2024).
[24] EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, https://www.facebook.com/business/news/Core-Audiences (last visited Jan. 12, 2024).
[25] ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494 (last visited Jan. 12, 2024).
[26] AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting (last visited Jan. 12, 2024).

information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[27]

68. Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences *only if they first supply Facebook with the underlying data*. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook's "Business Tools."[28]

69. As Facebook puts it, the Business Tools "help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[29]

---

[27] ABOUT LOOKALIKE AUDIENCES, https://www.facebook.com/business/help/164749007013531?id=401668390442328 (last visited Jan. 12, 2024).

[28] CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494; Facebook, Create a Website Custom Audience https://www.facebook.com/business/help/1474662202748341?id=2469097953376494 (last visited Jan. 12, 2024).

[29] THE FACEBOOK BUSINESS TOOLS, https://www.facebook.com/help/331509497253087 (last visited Jan. 12, 2024).

70. Put more succinctly, Facebook's Business Tools are bits of code that advertisers can integrate into their website, mobile applications, and servers, thereby enabling Facebook to intercept and collect user activity on those platforms.

71. The Business Tools are automatically configured to capture certain data, like when a User visits a webpage, that webpage's Universal Resource Locator ("URL") and metadata, or when a user downloads a mobile application or makes a purchase.[30]

72. Facebook's Business Tools can also track other events. Facebook offers a menu of "standard events" from which advertisers can choose, including what content a visitor views or purchases.[31] Advertisers can even create their own tracking parameters by building a "custom event." [32]

---

[30] *See* FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Apr. 19, 2024).

[31] SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited Apr. 19, 2024).

[32] ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/. (last visited Apr. 19, 2024),

73. One such Business Tool is the Meta Pixel. Facebook offers this code to advertisers, like Defendant, to integrate into their website. As the name implies, the Meta Pixel "tracks the people and type of actions they take."[33]

74. Meta pushes advertisers to install the Meta Pixel. Meta tells advertisers the Pixel "can help you better understand the effectiveness of your advertising and the actions people take on your site, like visiting a page or adding an item to their cart."[34]

75. Meta tells advertisers that the Meta Pixel will improve their Facebook advertising, including by allowing them to:

a. "measure cross-device conversions" and "understand how your cross-device ads help influence conversion.";

b. "optimize the delivery of your ads" and "[e]nsure your ads reach the people most likely to take action;" and

c. "create Custom Audiences from website visitors" and create "[d]ynamic ads [to] help you automatically show website visitors the products they viewed on your website—or related ones."[35]

---

[33] RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Jan. 11, 2024).

[34] Meta, Meta Pixel (2023), https://www.facebook.com/business/tools/meta-pixel.

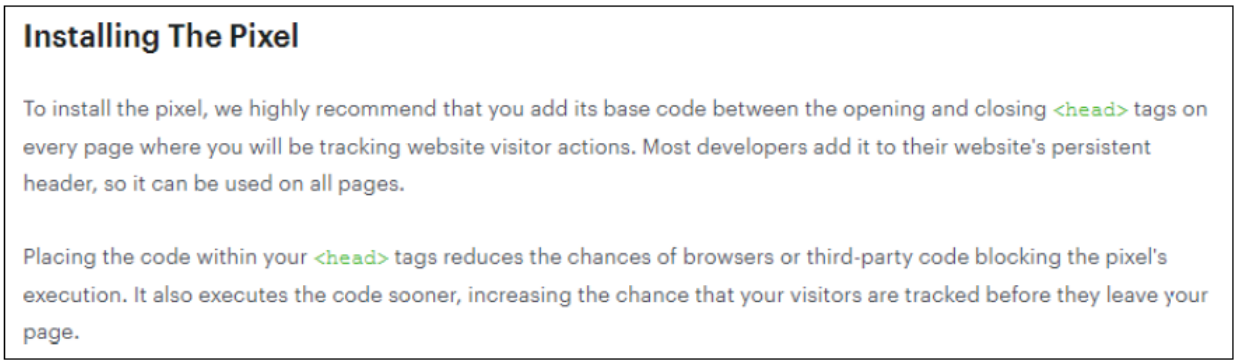
[35] *Id*.

76. Meta explains that the Meta Pixel "log[s] when someone takes an action on your website" such as "adding an item to their shopping cart or making a purchase," and the user's subsequent action:

Once you've set up the Meta Pixel, the Pixel will log when someone takes an action on your website. Examples of actions include adding an item to their shopping cart or making a purchase. The Meta Pixel receives these actions, or events, which you can view on your Meta Pixel page in Events Manager. From there, you'll be able to see the actions that your customers take. You'll also have options to reach those customers again through future Facebook ads.

77. The Meta Pixel is customizable. Meaning, web developers can choose the actions the Pixel will track and measure.

78. Meta advises web developers to place the Meta Pixel early in the source code for any given webpage or website to ensure that visitors will be tracked before they leave the webpage or website:



Installing The Pixel

To install the pixel, we highly recommend that you add its base code between the opening and closing <head> tags on every page where you will be tracking website visitor actions. Most developers add it to their website's persistent header, so it can be used on all pages.

Placing the code within your <head> tags reduces the chances of browsers or third-party code blocking the pixel's execution. It also executes the code sooner, increasing the chance that your visitors are tracked before they leave your page.

79. Meta also provides advertisers with step-by-step instructions for setting up and installing the Meta Pixel on their website, so that companies can add the Meta Pixel to their website without a developer.[36]

80. If a healthcare provider, such as Wellstar, installs the Meta Pixel code as Meta recommends, patients' actions on the provider's website are contemporaneously redirected to Meta. When a patient clicks a button to register for, or logs into or out of, a "secure" patient portal, Meta's source code commands the patient's computing device to send the content of the patient's communication to Meta while the patient is communicating with her healthcare provider—traveling directly from the user's browser to Facebook's server.

81. In other words, by design, Meta receives the content of a patient's portal log in communication immediately when the patient clicks the log-in button—even before the healthcare provider receives it.

[36] Meta, Meta Pixel (2023), https://www.facebook.com/business/tools/meta-pixel.

82. This contemporaneous, and secret transmission contains the original GET request sent to the host website, along with additional data that the Meta Pixel is configured to collect. This transmission is initiated by the Facebook code installed by Defendant and concurrent with the Users' communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendant's Web Properties—Defendant's own code, and the Facebook code Defendant embedded.

83. Thus, the Meta "pixel allows Facebook to be a silent third-party watching whatever you're doing."[37]

84. Wellstar, through its installation and use of the Meta Pixel, disclosed to Meta the content of patient communications while its patients were exchanging communications with Wellstar's Web Properties.

85. Wellstar's use of the Meta Pixel to send Facebook the names of patients' doctors would have permitted Wellstar to specifically target its existing patients with Facebook ads *based on their health conditions*, as well as create Lookalike Audiences for the same purpose. This could only be accomplished by

[37] Jefferson Graham, *Facebook spies on us but not by recording our calls. Here's how the social network knows everything*, USA Today (March 4, 2020 4:52 am), https://www.usatoday.com/story/tech/2020/03/04/facebook-not-recording-our-calls-but-has-other-ways-snoop/4795519002/#.

Wellstar disclosing to Meta the content of those patients' communications on Wellstar's Web Properties, providing Facebook with a list of Wellstar's patients, or otherwise disclosing the identity of Wellstar's patients to Meta through the Meta Collection Tools.

C. Defendant's Use of Source Code, the Meta Pixel & Interception of HTTP Requests.

86. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the Internet. Each "client device" (such as a computer, tablet or smartphone) accesses web content through a web browser (e.g., Google's Chrome, Mozilla's Firefox, Apple's Safari and Microsoft's Edge).

87. Every website is hosted by a computer "server" that holds the website's contents and through which the entity in charge of the website exchanges communications with Internet users' client devices via web browsers.

88. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- **HTTP Request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies.

- **Cookies**: a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are "third-party cookies" which means they can store and communicate data when visiting one website to an entirely different website.

- **HTTP Response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data. [38]

89. A patient's HTTP Request essentially asks the Website to retrieve certain information (such as the name of a doctor with whom a patient makes an appointment), and the HTTP Response renders or loads the requested information in the form of "Markup" (the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate the Web Properties).

90. Every website is comprised of Markup and "Source Code." Source Code is a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

91. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the

[38] One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses.

background without notifying the web browser's user. The Meta Pixel and other tracking technologies Wellstar uses constitute source code that does just that. These tracking technologies thus act much like a traditional wiretap.

92. Wellstar encourages customers to use its Web Properties to obtain healthcare services, such as making appointments with doctors and other providers and take other actions related to their personal health care. When interacting with Wellstar's Web Properties like this, Plaintiff and Class Members convey highly private and sensitive information to Wellstar.

93. When patients visit Wellstar's Web Properties via an HTTP Request to Wellstar's server, that server sends an HTTP Response including the Markup that displays the webpage visible to the user and Source Code, including Wellstar's Meta Pixel.

94. Thus, Wellstar, is in essence, handing patients a tapped device, and once the webpage is loaded into the patient's browser, the software-based wiretap is quietly waiting for private communications on the Web Properties to trigger the tap, which intercepts those communications intended only for Wellstar and transmits those communications to third parties, including Facebook.

95. Defendant intentionally configured the Meta Pixel installed on its Web Properties to capture both the "characteristics" of individual patients' communications with the Defendant's Web Properties (e.g., their IP addresses,

Facebook ID, cookie identifiers, device identifiers and account numbers) and the "content" of these communications (i.e., the buttons, links, pages, and tabs they click and view, as well as search terms entered into free text boxes and descriptive URLs showing the information being exchanged).

D. Meta Uses Identifiers to Match The Health Information It Collects With Facebook Users.

96. Meta uses cookies to identify patients, including cookies named c_user, datr, fr, and _fbp.

97. The c_user cookie identifies Facebook users. The c_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user account has one—and only one—unique c_user cookie. Meta uses the c_user cookie to record user activities and communications.

98. An unskilled computer user can obtain the c_user cookie value for any Facebook user by (1) going to the user's Facebook page, (2) right-clicking with their mouse, (3) selecting "View page source," (4) executing a control-f function for "UserID," and (5) copying the number value that appears after "UserID" in the page source code of the Facebook user's page.

99. Following these directions makes it possible to discover that the Facebook UserID assigned to Mark Zuckerberg is 4. By typing

www.facebook.com/4 into a browser and hitting enter, a browser directs to Mr. Zuckerberg's page at www.facebook.com/zuck.

100. A user's Facebook ID is therefore linked to their Facebook profile, which contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile. To find the Facebook account associated with a c_user cookie, one simply needs to type www.facebook.com/ followed by the c_user ID.

101. The Meta datr cookie identifies the web browser the patient is using. It is an identifier unique to each patient's specific web browser, so it is another way Meta can identify Facebook users.

102. Meta keeps a record of every datr cookie identifier associated with each of its users, and a Facebook user can obtain a redacted list of all datr cookies associated with his or her Facebook account from Meta by using the Facebook "Download Your Information" tool.

103. The Meta fr cookie is an encrypted combination of the c_user and datr cookies.[39]

104. The c_user, datar, and fr cookies are traditional third-party cookies, meaning they are cookies associated with a party other than the entity with which a person is communicating at the time. In the case of Wellstar, they are third-party cookies because Meta is a third party to the communication between a patient and their healthcare provider.

105. The Meta _fbp cookie is a Facebook identifier that is set by Facebook source code and associated with the healthcare provider using the Meta Pixel. (The letters fbp are an acronym for Facebook Pixel.)

106. The _fbp (or Facebook Pixel) cookie is also a third-party cookie in that it is also a cookie associated with Meta that is used by Meta to associate information about a person and their communications with non-Meta entities while the person is on a non-Meta website or application.

107. Meta disguises the _fbp cookie as a first-party cookie even though it is Meta's cookie on non-Meta websites.

---

[39] *See* Gunes Acar, *et al.*, Facebook Tracking Through Social Plug-ins: Technical Report Prepared for the Belgian Privacy Commission (Mar. 27, 2015), https://securehomes.esat.kuleuven.be/~ gacar/fb_tracking/fb_pluginsv1.0.pdf.

108. By disguising the _fbp cookie as a first-party cookie for a healthcare provider rather than a third-party cookie associated with Facebook, Meta ensures that the _fbp cookie is placed on the computing device of patients who seek to access the patient portal.

109. Healthcare providers with a patient portal require patients to enable first-party cookies to gain access to their patient records through the portal.

110. The purpose of these portal-associated first-party cookies is security. The _fbp cookie is then used as a unique identifier for that patient by Meta. If a patient takes an action to delete or clear third-party cookies from their device, the _fbp cookie is not impacted—even though it is a Meta cookie—again, because Meta has disguised it as a first-party cookie. Meta also uses IP address and user-agent information to match the health information it collects from Meta healthcare Partners with Facebook users.

111. Accordingly, Defendant's Web Properties through the Meta Pixel and other tracking technologies routinely provide Facebook with Defendant's patients' Facebook IDs, IP addresses, and/or device IDs and the other information they input into Defendant's Web Properties, including not only their medical searches, treatment requests, and the webpages they view, but also their name, email address, or phone number. This is precisely the type of identifying information that HIPAA

requires healthcare providers to anonymize to protect the privacy of patients.[40] Plaintiff's and Class Members' identities can be easily determined based on the Facebook ID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

112. After intercepting and collecting this information, Facebook processes it, analyzes it and assimilates it into datasets like Core Audiences and Custom Audiences. If the website visitor is also a Facebook user, the information collected via the Meta Pixel is associated with the user's Facebook ID that identifies their name and Facebook profile, i.e., their real-world identity.

113. While the Meta Pixel tool "hashes" personal data—obscuring it through a form of cryptography before sending the data to Facebook—that hashing does not prevent Facebook from reading, understanding, and using the data.[41] In fact, Facebook explicitly uses the hashed information it gathers to link Pixel-transmitted

---

[40] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Apr. 19, 2024).

[41] *See* https://www.facebook.com/business/help/112061095610075?id=2469097953376494; https://www.facebook.com/business/help/611774685654668?id=12053%2076682832142

data to Facebook profiles.[42] Indeed, there would be no value in targeting Facebook users with Defendant's ads if Facebook couldn't read the hashed data it received from Defendant to know *who* to target.

114. As Facebook explains, "[a]utomatic advanced matching will tell your pixel to look for recognizable form fields and other sources on your website that contain information such as first name, last name and email address. The Meta Pixel receives that information along with the event, or action, that took place. This information gets hashed in the visitor's browser. ***We can then use the hashed information to more accurately determine which people took action in response to your ad***."[43] Similarly, Facebook tells businesses: "When you upload your customer list in Ads Manager to create a Custom Audience, the information in your list is hashed before it's sent to Facebook. ***Facebook uses this hashed information and compares it to our own hashed information. Then, we help build your audience by***

---

[42] *See* https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

[43] https://www.facebook.com/business/help/611774685654668?id=120531207668283214 2

finding the Facebook profiles that match and create a Custom Audience for you from those matches."[44]

115. In other words, Facebook uses its own secret language to encode and then read and match individuals' information.

116. Facebook claims that after hashing individuals' Private Information (including their personal identifiers and PHI shared by Defendant) and matching it to Facebook profiles to create Custom Audiences, Facebook deletes the hashed data. Even assuming this is true, by that point, the damage is done—Facebook has read, understood, analyzed, and expressly taken action to match the shared PHI with specific individuals, with the express purpose of targeting those individuals with ads based on the data (PHI) that was shared and used to create Defendant's Custom Audiences—all at Defendant's request.

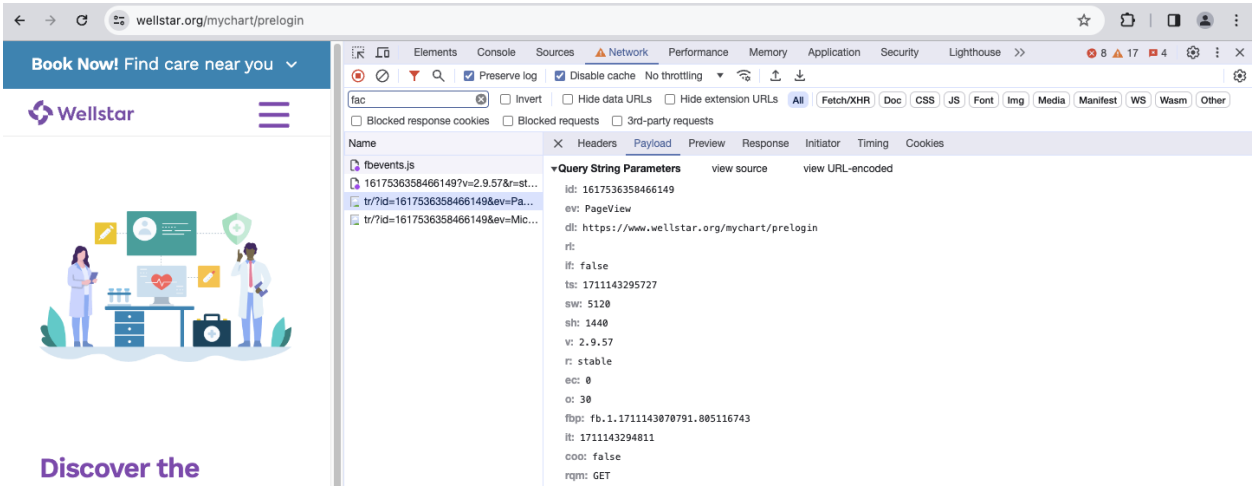
117. This disclosed PHI and PII allows Facebook to know that a specific patient is seeking confidential medical care and the type of medical care being sought, and in addition to permitting Defendant to target those persons with Defendant's ads, Facebook also then sells that information to marketers who will online target Plaintiff and Class Members.

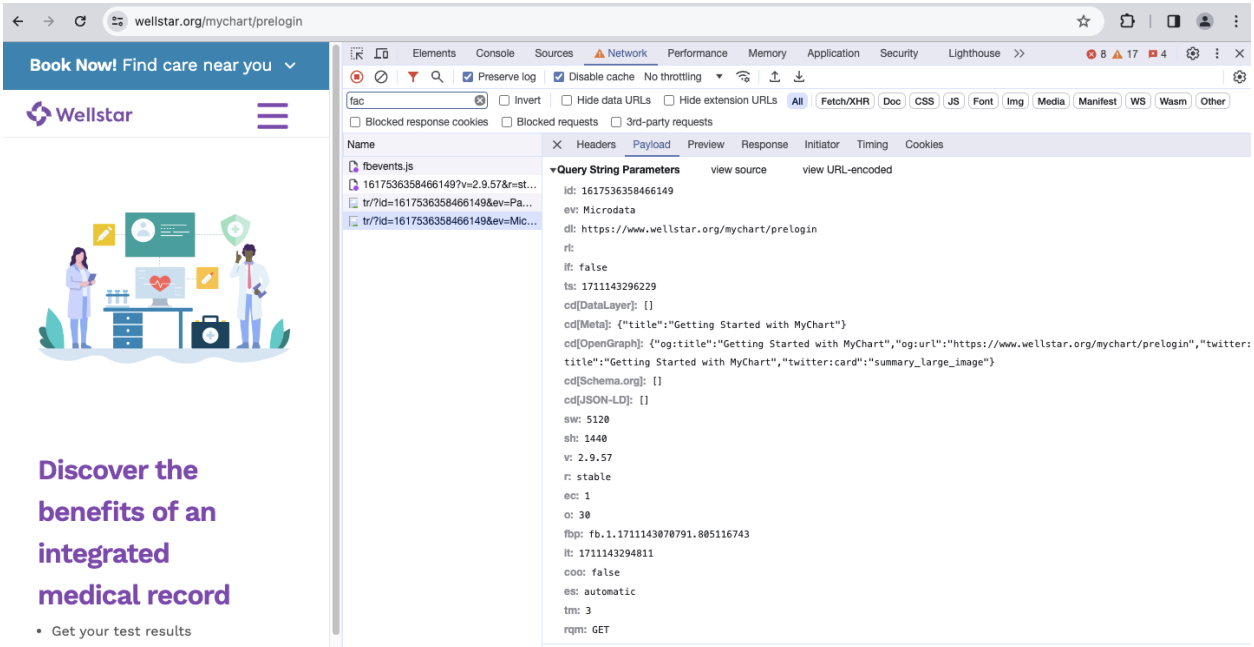
---

44 https://www.facebook.com/business/help/112061095610075?id=2469097953376494

E. Evidence that Wellstar Installed the Meta Pixel on its Web Properties and Used the Meta Pixel to Transmit Private Information to Meta.

118. A review of Wellstar's Web Properties shows the installation of the Meta Pixel with ID 1617536358466149:

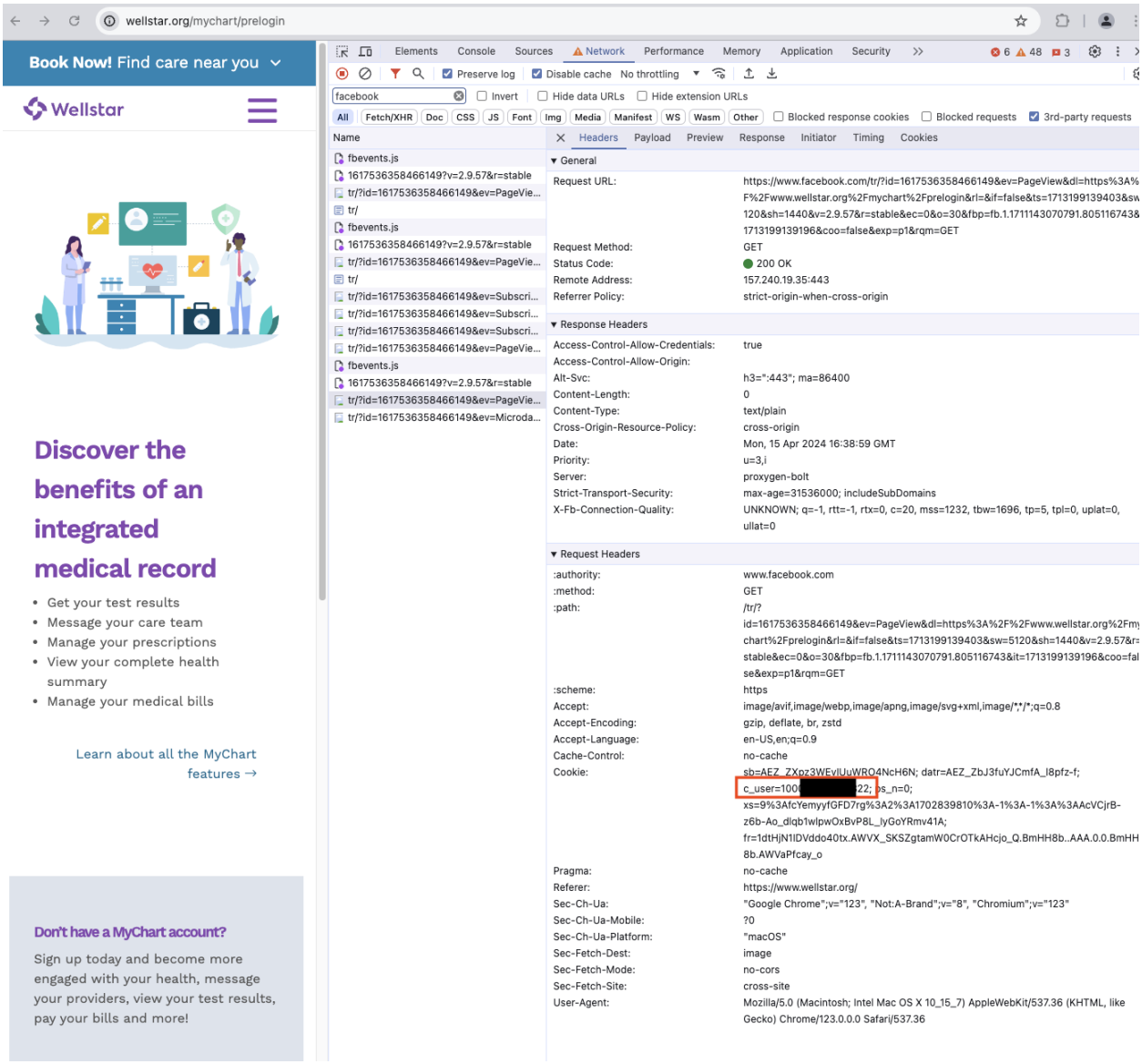




119. Archives of the Meta Pixel's configuration files demonstrate the actions that Wellstar took using the Meta Pixel that it installed and the custom events that it set up to transmit patients' Private Information to Meta.

120. Using the Pixel installed on its Web Properties, Wellstar transmitted PageView and Microdata events about Users' activities. Upon a User's arrival on Wellstar's homepage, Wellstar immediately sent a pair of PageView and Microdata events to Facebook revealing that the user was on the page, "https://www.Wellstar.org/." As Users navigated beyond the homepage, Wellstar continued to disclose user data including Users': (i) physician search activities; (ii) keyword search activities; (iii) appointment activities; (iv) Users' unique identifiers including their Facebook ID, names, or email addresses, and (v) MyChart and bill payment activities.

121. In each of the transmitted Meta Pixel events, Wellstar included the "c_user" cookie, which Facebook uses to identify Users:



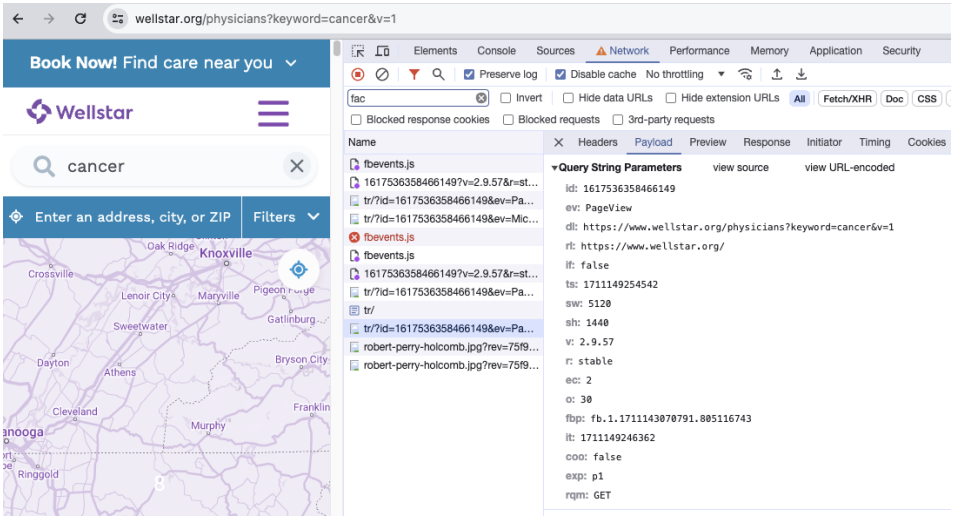
Cookie: sb=AEZ_ZXpz3WEvlUuWRO4NcH6N; datr=AEZ_ZbJ3fuYJCmfA_l8pfz-f; c_user=100[redacted]22; xs=9%3AfcYemyyfGFD7rg%3A2%3A1702839810%3A-1%3A-1%3A%3AAcVCjrB-z6b-Ao_dlqb1wlpwOxBvP8L_lyGoYRmv41A; fr=1dtHjN1lDVddo40tx.AWVX_SKSZgtamW0CrOTkAHcjo_Q.BmHH8b..AAA.0.0.BmHH8b.AWVaPfcay_o

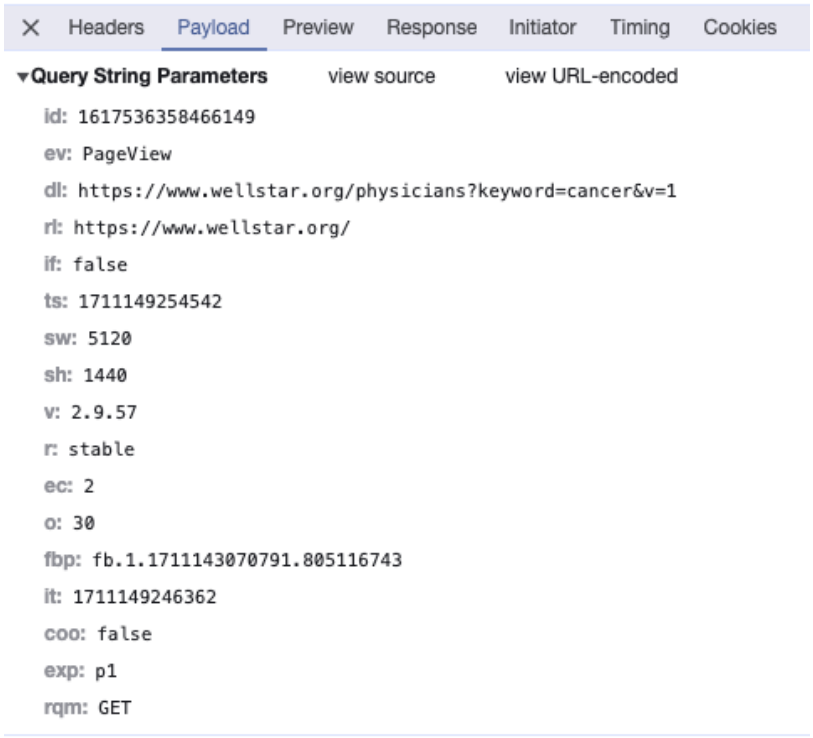
122. Therefore, Facebook could connect the cookie data that Wellstar transmitted with specified Users.

Wellstar Disclosed Users' Physician Search Activities

123. When a User searches Wellstar's Web Properties to find doctors, Wellstar sends a SubscribedButtonClick event informing Facebook that the User clicked to "Find a world-class physician" at https://www.wellstar.org/physicians. Wellstar then sent a further set of PageView and Microdata events when the User loaded the page on https://wellstar.org/physicians.

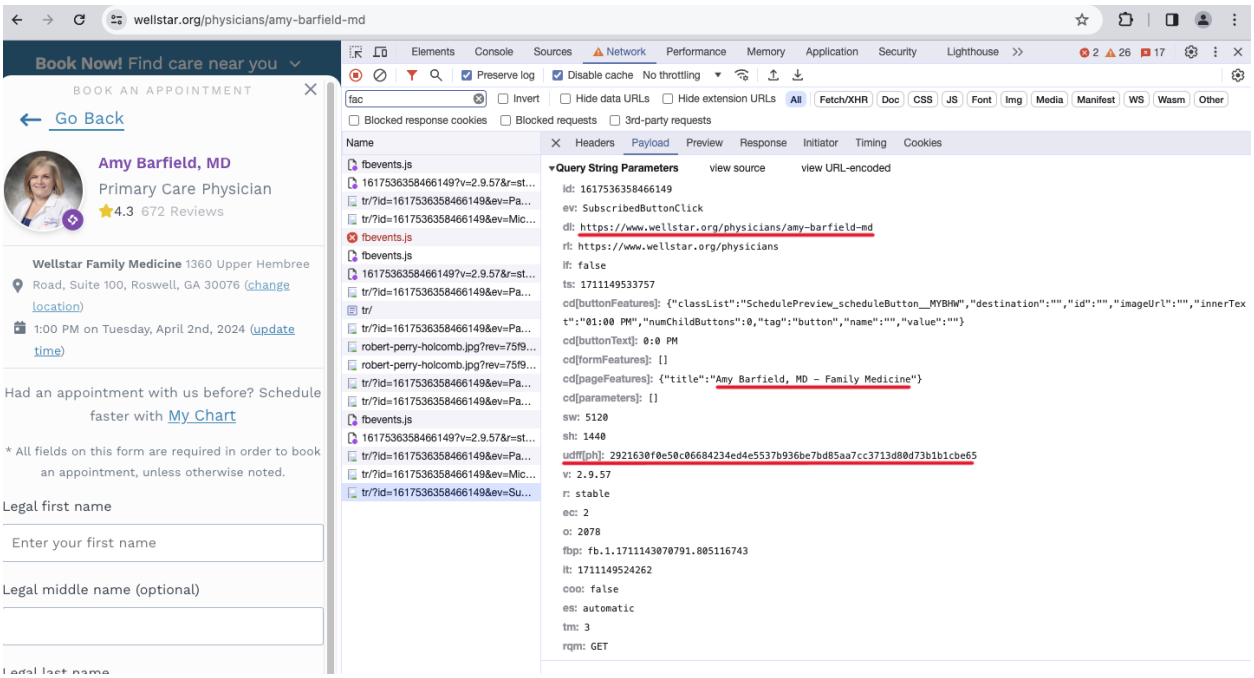
124. From the Physicians page, the User may search for a doctor by adding parameters such as specialty and location. Wellstar also sent Facebook such user parameters. As an example, when a user searched for a provider near Marietta, Georgia with a specialty of cancer, Wellstar sent PageView and Microdata events which reveal that the user searched for "physician" with the keyword "keyword=cancer".





125. Wellstar then discloses the User's activities as they interact with their search results. For instance, the User could click to view a physician's page, call a physician or book an appointment. As the User clicked for each action, Wellstar sent a SubscribedButtonClick event revealing the User's action and the context of the User's search for providers with a specialty of cancer in Marietta, Georgia.

126. Specifically, when the User clicked to view a physician's profile, the SubscribedButtonClick event Wellstar sent states the name of the provider and their specialty, for example, "Amy Barfield, MD – Family Medicine.":



127. Importantly, the SubscribedButtonClick events shown in the figure above includes the "udff[ph]" parameter, illustrating that Wellstar enabled **Advanced Matching Parameters**, which allow "Meta to connect collected event data to users, even if they do not have Facebook's browser cookies."[45] The "udff[ph]" parameter was ultimately transmitted to Meta, which included both the first and the last name of the User:

[45] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector#advanced-matching-parameters.

Wellstar Disclosed Users' Keyword Search Activities

128. Mirroring Wellstar's disclosures about Wellstar's physician search activities, Wellstar also shared information with Facebook about Users' physician search activities.

129. When a User searched for the keyword, cancer, for example, Wellstar reported that through PageView and Microdata events which included the User's "keyword=cancer."

130. Users could refine their keyword search results by filtering based on whether the result is for Wellstar's services, facilities, or doctors. Wellstar reported as Users filtered their results.

131. For example, when the User filtered their cancer search results to show only Wellstar's offered services, Wellstar sent a SubscribedButtonClick event. The event informs Facebook that the User clicked on "Services" on a search results page for "keyword=cancer."

132. The User could then browse and click through their filtered search results to learn more and conduct activities such as book appointments. Wellstar disclosed details as Users performed these actions.

133. For instance, when the User clicked to view more about Wellstar's cancer services, and then clicked to open a page about breast cancer, Wellstar sent a

series of SubscribedButtonClick, PageView, and Microdata events with details about the User's activities.

134. First, Wellstar transmitted SubscribedButtonClick, Pageview and Microdata events disclosing that the User clicked to open a page about Wellstar's cancer care services after conducting a query for cancer. Then, as the User navigated to learn about breast cancer services, Wellstar informed Facebook through PageView and Microdata events that the User navigated from a page with "keyword=cancer" to a page about "breast-cancer."

Wellstar Disclosed Users' Appointment Activities

135. Continuing the example immediately above, where a User conducted a search for cancer and then proceeded to learn about breast cancer, when the User clicked to schedule an appointment, Wellstar transmitted a SubscribedButtonClick event.

136. This event informs Facebook that the User clicked to "Schedule Appointment" which leads to "*https://www.wellstar.org/medical-services/health-conditions-diseases/breast-cancer*".

137. Wellstar also offered a more generalized appointment booking function on its website. Wellstar informed Facebook about Users' appointment activities there as well.

138. When a User clicked to "Book Appointment" on Wellstar's website, Wellstar sent a SubscribedButtonClick event divulging to Facebook that the User clicked "Book Appointment."

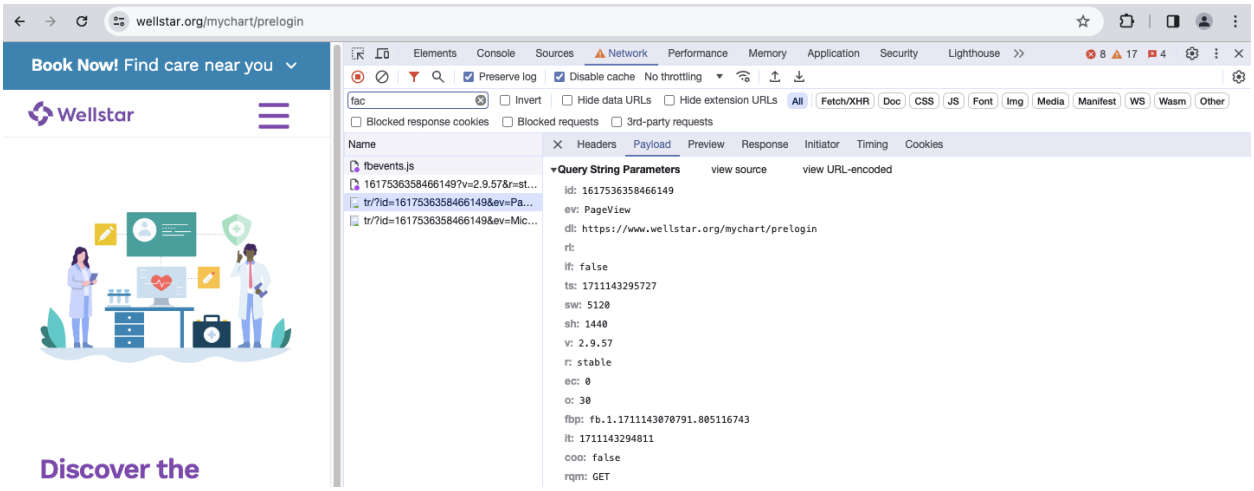
139. Wellstar then sent PageView and Microdata events confirming the User loaded the Physicians page. Once the User was on the Physicians page, Wellstar populated the page with a list of locations with which and physicians with whom the User can book an appointment. When the User clicked "Book Appointment," and then clicked a specific physician, Wellstar transmitted a SubscribedButtonClick event for each action disclosing the User's activities.

Wellstar Disclosed Users' MyChart Activities and Bill Pay Activities

140. Wellstar also disclosed User activities that reveal their status as current patients. Two examples of such activities are Users' MyChart and bill pay activities.

141. Upon a User's loading of the MyChart page, Wellstar informed Facebook that the User was on the page, "https://mychart.wellstar.org/mychart/Authentication/Login?" Importantly, this

shows that Wellstar installed its Meta Pixels directly on its MyChart patient portal login page:



142. From the MyChart page, the User could either click to sign into or sign up for a MyChart account. When the User did either, Wellstar sent a SubscribedButtonClick event informing Facebook that the User either clicked to "Sign in" or clicked to "Sign up" on "mychart/authentication/Login".

143. Similarly, when a guest User clicked to access the Pay Your Bill page, Wellstar informed Facebook that the User clicked "Pay Bill" to navigate to https://mychart.wellstar.org/MyChart/billing/guestpay/.

144. Subsequently, Wellstar transmitted PageView and Microdata events, confirming the User arrived on the page to "Pay as Guest".

145. If the User had questions about their bills, they could contact Wellstar customer support. When the User clicked to call Wellstar, Wellstar informed Facebook about this through a SubscribedButtonClick event. The event reveals that the User clicked to call "(470) 245-9989" on "https://www.wellstar.org/for-patients/pay-your-bill".

Wellstar Installed Third-Party Tracking Software *Inside* its MyChart Patient Portal

146. Plaintiff's investigation to-date revealed that Wellstar has been tracking patients' activities even *inside its MyChart patient portal*. Specifically, Wellstar installed Google Tag Manager ("GTM"), a Google tool for installing and managing tracking codes, inside the patient portal from at least March 16, 2021 through at least September 24, 2022. Discovery will help establish what specific tracking software Wellstar installed inside the patient portal and what information Wellstar was sharing with third parties via this software (in addition to the Meta Pixel on its Login and Pay Your Bill pages which revealed users' patient status to Facebook and likely other third parties). .[46] The tracking software that can be installed on a website using

[46] Google Tag Manager is used for managing and deploying marketing tags (tracking software) on a website without having to modify the code. *See* https://www.semrush.com/blog/google-tag-manager/

GTM include the Meta Pixel, Google Analytics and other Google marketing products.[47]

F. Wellstar's Privacy Policies & Promises.

147. Defendant's privacy policies represent to Plaintiff and Class Members that Defendant will keep Private Information private and confidential, and it will only disclose Private Information under certain circumstances.

148. Defendant publishes several privacy policies that represent to Users that Wellstar will keep sensitive information confidential and that it will only disclose PII and PHI provided to it under certain circumstances, none of which apply here.[48]

149. Defendant's separate Notice of Privacy Practices assures Plaintiff and Class Members that Wellstar is "required by law to protect the privacy of your health information."[49]

---

[47] *Id.*

[48] https://www.wellstar.org/financial-policy-and-privacy-info/internet-privacy-policy (last visited Apr. 12, 2024).

[49] https://www.wellstar.org/financial-policy-and-privacy-info/joint-notice-of-privacy-practices (last visited Apr. 12, 2024).

150. Defendant's Notice of Privacy Practices explains Defendant's duties with respect to IIHI and the exceptions for when Defendant can use and disclose Plaintiff's and Class Members' PHI in the following ways:

- For Treatment;
- For Payment;
- For Health Care Operations;
- To Provide You Information on Health Related Programs or Products;
- For Reminders;
- As required by Law;
- To Persons Involved With Your Care;
- For Public Health Activities;
- For Reporting Victims of Abuse, Neglect, or Domestic Violence;
- For Health Oversight Activities;
- For Judicial or Administrative Proceedings;
- For Law Enforcement Purposes
- To Avoid a Serious Threat to Health or Safety;
- For Specialized Government Functions;
- For Workers' Compensation;
- For Research Purposes;
- To Request Your Support;
- To Provide Information Regarding Decedents;
- For Organ Procurement Purposes;
- To Correctional Institutions or Law Enforcement Officials;
- To Business Associates;
- For Data Breach Notification Purposes; and
- Special Legal Protections for Certain Health Information.[50]

[50] *Id.*

151. Defendant also promises patients that "[a]ny sharing of your health information, other than as explained above, requires your written authorization."[51]

152. Defendant's privacy policy does not permit Defendant to use and disclose Plaintiff's and Class Members' IIHI for marketing purposes, stating that "we will not use your health information unless you authorize us in writing to: Share any of your psychotherapy notes, if they exist, with a third party; Share any of your health information with marketing companies; or Sell any of your health information."[52]

153. Notwithstanding these representations, Wellstar installed Meta's Collection Tools on its Web Properties and, thereafter, began to automatically transmit extensive IIHI from everyone who visited its Web Properties to Meta.

154. After receiving IIHI communicated on Wellstar's Web Properties, Meta analyzes and uses this information for its own commercial purposes that include building more fulsome profiles of its Users' preferences and traits and selling targeted advertisements based on this information. Meta also receives an additional commercial benefit from Wellstar's use of Meta's Collection Tools, namely that it

[51] *Id.*

[52] *Id.*

provides Wellstar with a greater incentive to advertise on Meta's social media platforms.

155. After receiving IIHI communicated on Wellstar's Web Properties, Meta forwards this data, and its analysis of this data, to Wellstar. Wellstar then uses this data and analysis for its own commercial purposes that include understanding how Users use its Website and determining what ads Users see on its Website.

156. At all times relevant to this Complaint, Wellstar did not notify Users that it automatically sends IIHI communicated on its Web Properties to Meta.

157. At all times relevant to this Complaint, Wellstar did not notify Users of its Web Properties that IIHI they communicate on its Web Properties were being used by Meta for commercial purposes.

158. At all times relevant to this Complaint, Wellstar did not notify Users of its Web Properties that it was using the IIHI they communicate on its Web Properties for commercial purposes.

159. Meta has not secured any informed consent or written permission allowing it to use IIHI communicated on Wellstar's Web Properties for commercial purposes.

160. Wellstar has not secured any informed consent or written permission allowing it to share IIHI communicated on its Web Properties with Meta or for commercial purposes.

161. Wellstar violated its own privacy policy by unlawfully intercepting and disclosing Plaintiff's and Class Members' Private Information to Facebook and third parties without adequately disclosing that it shared Private Information with third parties and without acquiring the specific patients' consent or authorization to share the Private Information.

DEFENDANT'S CONDUCT VIOLATES FEDERAL & STATE PRIVACY LAWS

A. The HIPAA Privacy Rule Protects Patient Healthcare Information.

162. Patient healthcare information in the United States is protected by federal law under HIPAA and its implementing regulations, which are promulgated by HHS.

163. The HIPAA Privacy Rule, located at 45 C.F.R. § 160 and 45 C.F.R. § 164 (A) and (E): "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to health plans, healthcare clearinghouses, and those healthcare providers that conduct certain healthcare transactions electronically."[53]

---

[53] The HIPAA Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html (last visited Apr. 19, 2024).

164. The Privacy Rule broadly defines PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

165. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse"; (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual"; and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

166. Under the HIPAA de-identification rule, "health information is not individually-identifiable only if: (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods and results of the analysis that justify such determination"; or (2) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed:

a. Names;

b. Medical record numbers;

c. Account numbers;

d. Device identifiers and serial numbers;

e. Web Universal Resource Locators (URLs);

f. Internet Protocol (IP) address numbers; … and

g. Any other unique identifying number, characteristic, or code…; and" the covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is subject of the information." 45 C.F.R. § 164.514.

167. The HIPAA Privacy Rule requires any "covered entity"—which includes healthcare providers like Wellstar—to maintain appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made of PHI without authorization. 45 C.F.R. §§ 160.103, 164.502.

168. An individual or corporation violates the HIPAA Privacy Rule if it knowingly: "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually-identifiable health information relating to an individual." The statute states that a "person … shall be considered to have obtained or disclosed individually-identifiable health information … if the information is maintained by a

covered entity … and the individual obtained or disclosed such information without authorization." 42 U.S.C. § 1320(d)(6).

169. The criminal and civil penalties imposed by 42 U.S.C. § 1320(d)(6) apply directly to Wellstar when it is knowingly disclosing IIHI relating to an individual, as those terms are defined under HIPAA.

170. Violation of 42 U.S.C. § 1320(d)(6) is subject to criminal penalties where "the offense is committed with intent to sell, transfer, or use individually-identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320(d)(6)(b). In such cases, an entity that knowingly obtains IIHI relating to an individual "shall be fined not more than $250,000, imprisoned not more than 10 years, or both." 42 U.S.C. § 1320(d)(6)(b)(1).

B. HIPAA Protects Patient Status Information.

171. HIPAA also protects against revealing an individual's status as a patient of a healthcare provider.

172. Guidance from HHS confirms that HIPAA protects patient status:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data.… **If such information was listed with health condition, healthcare provision or payment data, such as an indication that an individual was treated at a certain**

clinic, then this information would be PHI.[54]

173. HHS's guidance for marketing communications states that healthcare providers may not provide patient lists for marketing purposes without the consent of every included patient:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, **covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list**.[55]

174. HHS has previously instructed that the HIPAA Privacy Rule protects patient status:

> a. "The sale of a patient list to a marketing firm" is not permitted under HIPAA. 65 Fed. Reg. 82717 (Dec. 28, 2000);
>
> b. "A covered entity must have the individual's prior written authorization to use or disclose protected health

---

[54] Office for Civil Rights, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* at 5 (emphasis added) (Nov. 26, 2012), https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html.

[55] Marketing, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html

> information for marketing communications," which includes disclosure of mere patient status through a patient list. 67 Fed. Reg. 53186 (Aug. 14, 2002);
>
> c. It would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers." 78 Fed. Reg. 5642 (Jan. 25, 2013); and
>
> d. The only exception permitting a hospital to identify patient status without express written authorization is to "maintain a directory of individuals in its facility" that includes name, location, general condition, and religious affiliation when used or disclosed to "members of the clergy" or "other persons who ask for the individual by name." 45 C.F.R. § 164.510(1). Even then, patients must be provided an opportunity to object to the disclosure of the fact that they are a patient. 45 C.F.R. § 164.510(2).

C. HIPAA's Protections Do Not Exclude Internet Marketing.

175. As OCR reminded entities regulated under HIPAA (like Defendant) in its recently issued *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* bulletin:

> Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-***

> ***compliant authorizations, would constitute impermissible disclosures.***[56]

176. OCR makes it clear that information that is routinely collected by vendors on public-facing websites may be PHI, including unique identifiers such as IP addresses, device IDs or email addresses.[57]

177. HHS has also confirmed that healthcare providers violate HIPAA when they use tracking technologies that disclose an individual's identifying information (like an IP address) even if no treatment information is included and even if the individual does not have a relationship with the healthcare provider:

> This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (*i.e.* it is indicative that the individual has received or will receive healthcare services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or healthcare or payment for care. [58]

178. Further, HIPAA applies to healthcare providers' webpages with tracking technologies even outside the patient portal, i.e. to "unauthenticated" webpages:

> [T]racking technologies on unauthenticated webpages may access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and

---

[56] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, (emphasis added) (updated March 18, 2024) (last visited Apr. 19, 2024).

[57] *See id.*

[58] *Id.*

> disclosures to tracking technology vendors. Examples of unauthenticated webpages where the HIPAA Rules apply include: The login page of a regulated entity's patient portal (which may be the website's homepage or a separate, dedicated login page), or a user registration webpage where an individual creates a login for the patient portal … [and ***pages] that address[] specific symptoms or health conditions***, such as pregnancy or miscarriage, ***or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances***. For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a healthcare provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.[59]

179. **The HHS bulletin <u>reminds</u> covered entities, like Defendant, of its long-standing duty to safeguard PHI**, explicitly noting that "it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors," and proceeding to explain how online tracking technologies violate the same HIPAA privacy rules that have existed for decades.[60]

180. Disclosures of PHI for online marketing or sales purposes require patient authorization under HIPAA, which Defendant did not obtain here. *See* 45 CFR § 164.508(a)(3) ("a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the

---

[59] *Id*.

[60] *Id.* (emphasis added).

communication is in the form of: (A) a face-to-face communication made by a covered entity to an individual; or (B) a promotional gift of nominal value provided by the covered entity."); 45 CFR § 164.508(a)(4) ("a covered entity must obtain an authorization for any disclosure of protected health information which is a sale of protected health information, as defined in § 164.501 of this subpart [and] [s]uch authorization must state that the disclosure will result in remuneration to the covered entity.").

181. As a result, a healthcare provider like Defendant may not disclose PHI to a tracking technology vendor, like Meta, unless it has properly notified its Website Users and entered into a business associate agreement with the vendor in question.

182. Yet Defendant disclosed Plaintiff's and Class Members' PHI without their consent and without a business associate agreement with Meta.

D. Under HIPAA, IP Addresses are Personally Identifiable Information.

183. Through the use of the Meta Pixel, computer IP addresses are among the Private Information that was improperly disclosed to Facebook.

184. An IP address is a number that identifies the address of a device connected to the Internet.

185. IP addresses are used to identify and route communications on the Internet.

186. IP addresses of individual Internet users are used by Internet service providers, websites, and third-party tracking companies to facilitate and track Internet communications.

187. Facebook tracks every IP address ever associated with a Facebook user.

188. Google also tracks IP addresses associated with Internet users.

189. Facebook, Google, and other third-party marketing companies track IP addresses for use of tracking and targeting individual homes and their occupants with advertising by using IP addresses.

190. Under HIPAA, an IP address is considered PII:

a. HIPAA defines PII to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).

b. HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See* also, 45 C.F.R. § 164.514(b)(2)(i)(O).

191. Consequently, by disclosing Plaintiff's and Class Members' IP addresses, Defendant's business practices violated HIPAA and industry privacy standards.

E. The FTC Act Protects Health Information.

192. The FTC has made clear that "health information" is "anything that conveys information—or enables an information—about a consumer's health" and provides an example that location-data alone (such as repeated trips to a cancer treatment facility") "may convey highly sensitive information about a consumer's health."[61]

193. The FTC joined HHS in notifying HIPAA-covered entities and non-HIPAA-covered entities that sharing such "health information" with Google and Facebook is an unfair business practice under federal law:

> When consumers visit a hospital's website or seek telehealth services, they should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers' health information from potential misuse and exploitation."[62]

---

[61] Jillson, Elisa, *Protecting the privacy of health information: A baker's dozen takeaways from FTC cases*, Federal Trade Commission (July 25, 2023), *https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases*.

[62] *FTC and HHS Warn Hospital Systems and Telehealth Providers About Privacy and Security Risks from Online Tracking Technologies*, Federal Trade Commission (July 20, 2023), *https:// www.ftc.gov/news-events/news/press-releases/2023/07/ftc-*

F. Georgia Law Protects Health Information.

194. O.C.G.A. § 31-33-2 states that providers, which are defined to include hospitals, O.C.G.A. § 31-33-1, may only release medical records "upon written request from the patient or a person authorized to have access to the patient's record under an advance directive for health care, a psychiatric advance directive, or a durable power of attorney for health care for such patient," where "the record request [is] accompanied by: [a]n authorization in compliance with the federal Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. Section 1320d-2, et seq., and regulations implementing such act" and "a signed written authorization indicating that he or she is authorized to have access to the patient's records[.]"."

195. In addition, O.C.G.A. § 31-33-8 provides that health records in electronic format are "subject to all applicable federal laws governing the security and confidentiality of a patient's personal health information."

196. Thus, Georgia law requires all hospitals, including Wellstar, to maintain all medical records and information within their control as confidential, rendering Wellstar's actions with respect to the interception and disclosure of its patients' Private Information to Meta unlawful under Georgia law.

---

hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking.

G. Wellstar Violated Industry Standards.

197. A medical provider's duty of confidentiality is embedded in the physician-patient and hospital-patient relationship, it is a cardinal rule.

198. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

199. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care… Patient privacy encompasses a number of aspects, including, … personal data (informational privacy)

200. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

201. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically…must…:(c) release patient information only in keeping ethics guidelines for confidentiality.

H. Plaintiff's & Class Members' Expectations of Privacy

202. Plaintiff and Class Members were aware of Wellstar's duty of confidentiality when they sought medical services from Wellstar.

203. Indeed, at all times when Plaintiff and Class Members provided their PII and/or PHI to Wellstar, they each had a reasonable expectation that the information would remain private and that Wellstar would not share their Private Information with third parties for a commercial purpose, unrelated to patient care.

204. Privacy polls and studies show that the overwhelming majority of Americans consider obtaining an individual's affirmative consent before a company collects and shares its customers' data to be one of the most important privacy rights.

205. For example, a recent Consumer Reports study shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumer data, and the same percentage believe

those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.[63]

206. Personal data privacy and obtaining consent to share Private Information are material to Plaintiff and Class Members.

207. Plaintiff's and Class Members' reasonable expectations of privacy in their Private Information are grounded in, among other things, Defendant's status as a healthcare provider, Defendant's common law obligation to maintain the confidentiality of patients' Private Information, state and federal laws protecting the confidentiality of medical information, state and federal laws protecting the confidentiality of communications and computer data, state laws prohibiting the unauthorized use and disclosure of personal means of identification, and Defendant's express and implied promises of confidentiality.

I. Patients Have Protectable Property Interests in Their IIHI.

208. Property is the right of any person to possess, use, enjoy or dispose of a thing, including intangible things like data and communications. Plaintiff and Class Members have a vested property right in their IIHI.

---

[63] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, (May 11, 2017), available at https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/ (last visited Apr. 19, 2024).

209. Federal and state laws grant patients the right to protect the confidentiality of data that identifies them as patients of a particular healthcare provider and restrict the use of their health data, including their status as a patient, to only uses related to their care or otherwise authorized by federal or state law in the absence of patient authorization.

210. A patient's right to protect the confidentiality of their health data and restrict access to this data is valuable.

211. In addition, patients enjoy property rights in the privacy of their health communications under statutes such as HIPAA. State health privacy laws and American courts have also long recognized common law property rights in the content of a person's communications that are not to be used or disclosed to others without authorization.

212. Property rights in communications and information privacy are established by:

a. The Electronic Communications Privacy Act, including Title I (the Wiretap Act); Title II (the Stored Communications Act); and Title III (the Pen Register Act); and

b. Common law information property rights regarding the exclusive use of confidential information that have existed for centuries and continue to exist, s*ee Folsom v. Marsh*, 9 F.Cas. 342, 346 (C.C.D. Mass. 1841) (Story, J); *Baker v. Libbie*, 210 Mass. 599, 602 (1912); *Denis v. LeClerc*, 1 Mart. (La.) 297 (1811).

213. Meta's CEO, Mark Zuckerberg, has acknowledged that Meta users have an ownership interest in their data. In 2010, when Meta first revealed its "Download Your Information" tool, Zuckerberg stated that, "People own and have control over all info they put into Facebook and 'Download Your Information' enables people to take stuff with them."[64] Although Zuckerberg's statements regarding people's ability to "control" the information "put into Facebook" and the ability to access all such data via DYI is not true, his statement about data ownership is true.

214. Wellstar's unauthorized interception and disclosure of Plaintiff's and Class Members' IIHI violated their property rights to control how their data and communications are used and who may be the beneficiaries of their data and communications.

J. The Information Wellstar Discloses to Meta Without Plaintiff's or Class Members' Consent Has Actual, Measurable Monetary Value.

215. After receiving IIHI communicated on Wellstar's Web Properties, Meta forwards its analysis of this data to Wellstar. Wellstar then uses that analysis

---

64 https://techcrunch.com/2010/10/06/facebook-now-allows-you-to-download-your-information/.

for its own commercial purposes, including to target ads at existing patients or other people with characteristics similar to certain groups of Users.

216. Technology companies are under particular scrutiny because they already have access to a massive trove of information about people, which they use to serve their own purposes, including potentially micro-targeting advertisements to people with certain health conditions.

217. Meta "generate[s] substantially all of [its] revenue from advertising."[65]

218. Meta annually receives billions of dollars of unearned advertising sales revenue from Meta healthcare Partners, including Wellstar, who are targeting Facebook users based on their health information.

219. The robust market for Internet user data has been analogized to the "oil" of the tech industry.[66] A 2015 article from TechCrunch accurately noted that "[d]ata has become a strategic asset that allows companies to acquire or maintain a competitive edge."[67]

---

[65] Meta 2022 Annual Report at 17.

[66] *See* https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last visited Apr. 19, 2024).

[67] *See* https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/ (last visited Jan. 9, 2024).

220. That article noted that the value of a single Internet user—or really, a single user's data—varied from about $15 to more than $40.

221. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data (after costs).[68] At the time, estimates for 2022 were as high as $434 per user, for a total of more than $200 billion industry wide.

222. Professor Paul M. Schwartz, writing in the Harvard Law Review, notes: "Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information."[69]

223. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis and use. However, the data also has economic value to Internet users. Market exchanges have sprung up where

---

[68] *See What Your Data is Really Worth to Facebook* (Jul. 12, 2019), https://washingtonmonthly.com/2019/07/12/what-your-data-is-really-worth-to-facebook/ (last visited Apr. 19, 2024).

[69] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2056-57 (2004).

individual users like Plaintiff herein can sell or monetize their own data. For example, Nielsen Data and Mobile Computer will pay Internet users for their data.[70]

224. There are countless examples of this kind of market, which is growing more robust as information asymmetries are diminished through revelations to users as to how their data is being collected and used.

225. Courts recognize the value of personal information and the harm when it is disclosed without consent. *See, e.g., In re Facebook Privacy Litig*., 572 F. App'x 494, 494 (9th Cir. 2014) (holding that plaintiffs' allegations that they were harmed by the dissemination of their personal information and by losing the sales value of that information were sufficient to show damages for their breach of contract and fraud claims); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig*., 440 F. Supp. 3d 447, 462 (D. Md. 2020) (recognizing "the value that personal identifying information has in our increasingly digital economy").

226. Healthcare data is particularly valuable on the black market because it often contains all of an individual's PII and medical conditions as opposed to a single piece of information that may be found in a financial breach.

---

[70] *See 10 Apps for Selling Your Data for Cash*, https://wallethacks.com/apps-for-selling-your-data/ (last visited Jan. 9, 2024).

227. Healthcare data is incredibly valuable because, unlike a stolen credit card that can be easily canceled, most people are unaware that their medical information has been sold. Once it has been detected, it can take years to undo the damage caused.

228. The value of health data is well-known and various reports have been conducted to identify its value.

229. Specifically, in 2023, the Value Examiner published a report entitled Valuing Healthcare Data. The report focused on the rise in providers, software firms and other companies that are increasingly seeking to acquire clinical patient data from healthcare organizations. The report cautioned providers that they must de-identify data and that purchasers and sellers of "such data should ensure it is priced at fair market value to mitigate any regulatory risk."[71]

230. Trustwave Global Security published a report entitled The Value of Data. With respect to healthcare data records, the report found that they may be

[71] *See* https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf (last visited Apr. 19, 2024).

valued at up to $250 per record on the black market, compared to $5.40 for the next highest value record (a payment card).[72]

231. The value of health data has also been reported extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry," in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[73]

232. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[74]

233. The dramatic difference in the price of healthcare data compared to other forms of private information commonly sold is evidence of the value of PHI.

---

[72] *See* https://www.imprivata.com/blog/healthcare-data-new-prize-hackers (last visited Jan. 9, 2024) (citing https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf).

[73] *See* https://time.com/4588104/medical-data-industry/ (last visited Apr. 19, 2024).

[74] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited Apr. 19, 2024).

234. These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users' stolen data, surely Internet users can sell their own data.

235. In short, there is a quantifiable economic value to Internet users' data that is greater than zero. The exact number will be a matter for experts to determine.

K. Defendant was Enriched & Benefitted from the Use of The Meta Pixel & Unauthorized Disclosures.

236. Defendant installed the Meta Collection Tools on its Web Properties to benefit its own marketing and revenue.

237. In exchange for disclosing the PII of its patients, Defendant is compensated by Facebook in the form of enhanced advertising services and more cost-efficient marketing on Facebook.

238. Retargeting is a form of online marketing that targets users with ads based on their previous Internet communications and interactions. In particular, retargeting operates through code and tracking pixels placed on a website and cookies to track website visitors and then places ads on other websites the visitor goes to later.[75]

[75] *The complex world of healthcare retargeting*, https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting/ (last visited Apr. 19, 2024).

239. The process of increasing conversions and retargeting occurs in the healthcare context by sending a successful action on a healthcare website back to Facebook via the tracking technologies and the Meta Pixel embedded on, in this case, Wellstar's Web Properties. For example, when a User searches for doctors or medical conditions or treatment on Wellstar's Web Properties, that information is sent to Facebook. Facebook can then use its data on the User to find more users to click on a Wellstar ad and ensure that those Users targeted are more likely to convert.[76]

240. Through this process, the Meta Pixel loads and captures as much data as possible when a User loads a healthcare website that has installed the Pixel. The information the Pixel captures, "includes URL names of pages visited, and actions taken—all of which could be potential examples of health information."[77]

241. Plaintiff's and Class Members' Private Information has considerable value as highly monetizable data especially insofar as it allows companies to gain insight into their customers so that they can perform targeted advertising and boost their revenues.

---

[76] *See, e.g.*, *How to Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking* (Mar. 14, 2023), *https://www.freshpaint.io/blog/how-to-make-facebook-ads-hipaa-compliant-and-still-get-conversion-tracking* (last visited Apr. 19, 2024).

[77] *Id.*

242. In exchange for disclosing the Private Information of their account holders and patients, Wellstar is compensated in the form of enhanced advertising services and more cost-efficient marketing on its platform.

243. But companies have started to warn about the potential HIPAA violations associated with using pixels and tracking technologies because many such trackers are not HIPAA-compliant or are only HIPAA-compliant if certain steps are taken.[78]

244. For example, Freshpaint, a healthcare marketing vendor, cautioned that "Meta isn't HIPAA-compliant. They don't sign BAAs, and the Meta Pixel acts like a giant personal user data vacuum sending PHI to Meta servers," and "[i]f you followed the Facebook (or other general) documentation to set up your ads and conversion tracking using the Meta Pixel, remove the Pixel now."[79]

245. Meta's Terms of Service, Data Policy, and Cookies Policy neither inform Facebook users that Meta may acquire their health information when they

---

[78] *See The guide to HIPAA compliance in analytics*, https://campaign.piwik.pro/wp-content/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf (explaining that Google Analytics 4 is not HIPAA-compliant) (last visited Jan. 9, 2024).

[79] *How To Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking*, *supra*, n.76.

interact with healthcare providers' websites and applications, nor obtain their consent for any such acquisitions.

246. Medico Digital also warns that "retargeting requires sensitivity, logic and intricate handling. When done well, it can be a highly effective digital marketing tool. But when done badly, it could have serious consequences."[80]

247. Whether a User has a Facebook profile is not indicative of damages because Facebook creates shadow profiles, and at least one court has recognized that the Meta Pixel's ability to track comprehensive browsing history is also relevant. *See, e.g.*, *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1078–79 (N.D. Cal. 2021) (finding a reasonable expectation of privacy where Google combined the unique identifier of the user it collects from websites and Google Cookies that it collects across the internet on the same user).

248. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients to get more patients connected to the Wellstar MyChart portal.

249. By utilizing the Meta Pixel, the cost of advertising and retargeting was reduced, thereby benefiting Defendant.

---

[80] *The complex world of healthcare retargeting, supra,* n.75.

REPRESENTATIVE PLAINTIFF'S EXPERIENCE

A. Plaintiff Jane Doe's Experience

250. Plaintiff Jane Doe entrusted her Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff disclosed her Private Information to Defendant.

251. On numerous occasions, from at least May 2013 to present, Plaintiff accessed mychart.wellstar.org and Defendant's Website on her mobile device and/or computer to receive healthcare services from Defendant and at Defendant's direction.

252. Plaintiff used Defendant's Web Properties, including Wellstar's MyChart, multiple times per year to, among other things, make appointments with doctors, exchange messages with her doctors, fill out questionnaires requested by her doctors, request referrals for specific health issues, refill prescriptions, update medication information, and check medical test results.

253. Plaintiff has been diagnosed with chronic conditions, such as high blood pressure and high cholesterol. Plaintiff submitted information to Defendant's Web Properties about each of these medical conditions. For example, in 2016 and 2022, Plaintiff exchanged messages on Defendant's Web Properties about increasing and decreasing the dosages of various medications to treat these conditions, including Metoprolol and Atorvastatin.

254. Plaintiff has also been diagnosed with acute conditions, including an abscess on a certain region of her posterior that required surgery in 2017. In 2022, Plaintiff used Defendant's Web Properties to send a message to her primary care physician at Wellstar about the abscess, as it had reformed, and Plaintiff sought a referral for another surgery. Plaintiff's PCP responded on Defendant's Web Properties by referring Plaintiff to the same surgeon to evaluate her condition.

255. In 2022, Plaintiff exchanged messages with her care team on Defendant's Web Properties about chest pain, trouble sleeping, and various medical interventions to treat the same. That same year, Plaintiff also received and viewed referrals to Neurology, Cardiology, General Surgery, and Physical Therapy on Defendant's Web Properties.

256. Plaintiff has frequently used Defendant's Web Properties to check for test results for at least 56 lab tests since June 2016, including tests for cancer and Hepatitis C.

257. Plaintiff has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case.

258. Plaintiff read Defendant's Notice of Privacy Practices concerning the circumstances under which Defendant would share her health information when she first became a patient of Defendant and each time the policy was presented for her to read and sign.

259. Plaintiff provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

260. Plaintiff reasonably expected that her communications with Defendant via the Web Properties were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

261. Pursuant to the systematic process described herein, Wellstar assisted Meta with intercepting Plaintiff's communications, including those that contained PII, PHI and related confidential information.

262. Defendant transmitted to Meta Plaintiff's Facebook ID, computer IP address, and information relating to her medical conditions, including test results.

263. Wellstar assisted these interceptions without Plaintiff's knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff's PII and/or PHI.

264. Defendant did not inform Plaintiff that it had shared her Private Information with Meta.

265. Plaintiff suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of her Private Information; (iii) loss of benefit of the

bargain; (iv) diminution of value of the Private Information; (v) statutory damages and (v) the continued and ongoing risk to her Private Information.

266. Plaintiff is an active patient of Wellstar and seeks to continue to use the Web Properties to view her test results and communicate other Private Information concerning her medical conditions with Wellstar, but fears that without court action, her Private Information will be shared with unauthorized third parties, such as Meta, in the future.

267. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future unauthorized disclosure.

TOLLING

268. Any applicable statutes of limitation have been tolled by Defendant's knowing and active concealment of its incorporation of the Meta Pixel into its Web Properties.

269. The Meta Pixel and other tracking tools on Defendant's Web Properties were and are entirely invisible to a Web Properties visitor.

270. Through no fault or lack of diligence, Plaintiff and Class Members were deceived and could not reasonably discover Defendant's deception and unlawful conduct.

271. Plaintiff was ignorant of the information essential to pursue her claims, without any fault or lack of diligence on her part.

272. Defendant had exclusive knowledge that its Web Properties incorporated the Meta Pixel and other tracking tools and yet failed to disclose to its patients, including Plaintiff and Class Members, that by seeking medical care through Defendant's Website, Plaintiff's and Class Members' Private Information would be disclosed or released to Facebook and other unauthorized third parties.

273. Under the circumstances, Defendant was under a duty to disclose the nature, significance, and consequences of its collection and treatment of its patients' Private Information. In fact, to the present, Defendant has not conceded, acknowledged, or otherwise indicated to its patients that it has disclosed or released their Private Information to unauthorized third parties. Accordingly, Defendant is estopped from relying on any statute of limitations.

274. Moreover, all applicable statutes of limitation have also been tolled pursuant to the discovery rule.

275. The earliest that Plaintiff or Class Members, acting with due diligence, could have reasonably discovered Defendant's conduct would have been shortly before the filing of this suit.

CLASS ACTION ALLEGATIONS

276. Plaintiff brings this action individually and on behalf of all other persons similarly situated ("the Class") pursuant to Fed. R. Civ. P. 23.

277. The nationwide Class that Plaintiff seeks to represent is defined as follows:

> All persons residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the Meta Collection Tools on Defendant's Web Properties.

278. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

279. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

280. **Numerosity, Fed. R. Civ. P. 23(a)(1):** The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are millions of individuals whose PII and PHI may have been improperly accessed by Facebook, and the Class is identifiable within Defendant's records.

281. **Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3):** Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant violated its Privacy Policies by disclosing the Private Information of Plaintiff and Class Members to Facebook and/or additional third parties;

d. Whether Defendant adequately, promptly and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to third parties;

e. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

f. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient Private Information;

g. Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

h. Whether Defendant violated the consumer protection statutes invoked herein;

i. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

j. Whether Defendant knowingly made false representations as to its data security and/or Privacy Policy practices;

k. Whether Defendant knowingly omitted material representations with respect to its data security and/or Privacy Policies practices; and

l. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm they face as a result of Defendant's disclosure of their Private Information.

282. **Typicality, Fed. R. Civ. P. 23(a)(3):** Plaintiff's claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of Defendant's incorporation of the Meta Pixel, due to Defendant's misfeasance.

283. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully disclosed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy. Defendant's policies challenged herein apply to and affect Class Members uniformly, and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

284. **Adequacy of Representation, Fed. R. Civ. P. 23(a)(4):** Plaintiff will fairly and adequately represent and protect the interests of Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of

the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class, and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

285. **Superiority and Manageability, Fed. R. Civ. P. 23(b)(3):** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

286. **Policies Generally Applicable to the Class.** This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition

of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly, and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

287. The nature of this action and the nature of laws available to Plaintiff and Class Members makes the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

288. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable

identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

289. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

290. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and Defendant may continue to act unlawfully as set forth in this Complaint.

291. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

292. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information;

b. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information with respect to Defendant's privacy policy;

c. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

d. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

e. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to third parties;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;

g. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CLAIMS FOR RELIEF

COUNT I

INVASION OF PRIVACY— INTRUSION UPON SECLUSION
(On Behalf of Plaintiff & the Class)

293. Plaintiff repeats the allegations contained in the foregoing paragraphs preceding this Counts Section as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

294. Plaintiff and Class Members had a legitimate expectation of privacy regarding their PII and PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

295. Defendant owed a duty to Plaintiff and Class Members to keep their PII and PHI confidential.

296. The unauthorized disclosure and/or acquisition by a third party of Plaintiff's and Class Members' PII and PHI is highly offensive to a reasonable person.

297. Defendant's willful and intentional disclosure of Plaintiff's and Class Members' PII and PHI constitutes an intentional interference with Plaintiff's and Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

298. Defendant's conduct constitutes an intentional physical or sensory intrusion on Plaintiff's and Class Members' privacy because Defendant facilitated Facebook's simultaneous eavesdropping and wiretapping of confidential communications.

299. Defendant failed to protect Plaintiff's and Class Members' Private Information and acted with a knowing state of mind when it incorporated the Meta Pixel into its website because it knew the functionality and purpose of the Meta Pixel.

300. Because Defendant intentionally and willfully incorporated the Meta Pixel into its Web Properties and encouraged patients to use those Web Properties for healthcare purposes, Defendant had notice and knew that its practices would cause injury to Plaintiff and Class Members.

301. As a proximate result of Defendant's acts and omissions, the private and sensitive PII and PHI of Plaintiff and Class Members was disclosed to a third party without authorization, causing Plaintiff and the Class to suffer damages.

302. Plaintiff, individually and on behalf of the Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, loss of time and opportunity costs, punitive damages, plus prejudgment interest, and costs.

303. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII and PHI are still maintained by Defendant and still in the possession of Facebook and the wrongful disclosure of the information cannot be undone.

304. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not undo Defendant's disclosure of the information to Facebook, who on information and belief continues to possess and utilize that information.

305. Plaintiff, individually and on behalf of the Class Members, further seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' PII and PHI and to adhere to its common law, contractual, statutory, and regulatory duties.

COUNT II

BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff & the Class)

306. Plaintiff repeats the allegations contained in the foregoing paragraphs preceding this Counts Section as if fully set forth herein and bring this claim individually and on behalf of the proposed Class.

307. In light of the special relationship between Defendant Wellstar and Plaintiff and Class Members, whereby Defendant Wellstar became a guardian of Plaintiff's and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members; (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of an unauthorized disclosure and (3) to maintain complete and accurate records of what information (and where) Defendant Wellstar did and does store.

308. Defendant Wellstar has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant Wellstar's relationship with its patients and former patients, in particular, to keep secure their Private Information.

309. Defendant Wellstar breached its fiduciary duties to Plaintiff and Class Members by disclosing their Private Information to unauthorized third parties, and separately, by failing to notify Plaintiff and Class Members of this fact.

310. Defendant's breach of fiduciary duty was a legal cause of damage to Plaintiff and Class Members.

311. But for Defendant's breach of fiduciary duty, the damage to Plaintiff and Class Members would not have occurred.

312. As a direct and proximate result of Defendant Wellstar's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer injury and are entitled to compensatory, nominal, and/or punitive damages and disgorgement of ill-gotten gains, in an amount to be proven at trial.

COUNT III

NEGLIGENCE
(*On Behalf of Plaintiff & the Class*)

313. Plaintiff repeats the allegations contained in the foregoing paragraphs preceding this Counts Section as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

314. Defendant Wellstar required Plaintiff and Class Members to submit non-public personal information in order to obtain healthcare services.

315. Upon accepting, storing and controlling the Private Information of Plaintiff and the Class in its computer systems, Defendant owed, and continues to owe, a duty to Plaintiff and the Class to exercise reasonable care to secure, safeguard and protect their highly sensitive Private Information from disclosure to third parties.

316. Defendant breached its duty by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

317. It was reasonably foreseeable that Defendant's failures to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information through its installation and use of the Meta Pixels and other tracking technologies would result in unauthorized third parties, such as Meta, gaining access to such Private Information for no lawful purpose.

318. Defendant's duty of care to use reasonable measures to secure and safeguard Plaintiff's and Class Members' Private Information arose due to the special relationship that existed between Defendant and its patients, which is recognized by statute, regulations, and the common law.

319. Defendant Wellstar's duty to use reasonable care in protecting confidential data arose also because Defendant is bound by industry standards to protect confidential Private Information.

320. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their Private Information.

321. Defendant's misconduct included the failure to (1) secure Plaintiff's and Class Members' Private Information; (2) comply with industry standard data security practices; (3) implement adequate website and event monitoring; (4) implement the systems, policies, and procedures necessary to prevent unauthorized disclosures resulting from the use of the Meta Pixels and other tracking technologies and (5) prevent unauthorized access to Plaintiff's and Class Members' Private

Information by sharing that information with Meta and other third parties. Defendant's failures and breaches of these duties constituted negligence.

322. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and Class members' Private Information, Plaintiff and the Class have suffered damages that include, without limitation, loss of the benefit of the bargain, increased infiltrations into their privacy through spam and targeted advertising they did not ask for, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

323. Defendant's wrongful actions and/or inactions and the resulting unauthorized disclosure of Plaintiff's and Class members' Private Information constituted (and continue to constitute) negligence at common law.

324. Plaintiff and Class Members are entitled to compensatory, nominal, and/or punitive damages, and Plaintiff and Class Members are entitled to recover those damages in an amount to be determined at trial.

325. Defendant Wellstar's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner. Therefore, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant Wellstar to (i) strengthen its data security systems and monitoring procedures; (ii) cease sharing Plaintiff's and Class Members' Private

Information with Facebook and other third parties without Plaintiff's and Class Members' express consent and (iii) submit to future annual audits of its security systems and monitoring procedures.

COUNT IV

NEGLIGENCE PER SE
(*On Behalf of Plaintiff & the Class*)

326. Plaintiff repeats the allegations contained in the foregoing paragraphs preceding this Counts Section as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

327. Defendant Wellstar required Plaintiff and Class Members to submit non-public personal information in order to obtain healthcare services.

328. Upon accepting, storing and controlling the Private Information of Plaintiff and the Class in its computer systems, Defendant owed, and continues to owe, a duty to Plaintiff and the Class to exercise reasonable care to secure, safeguard and protect their highly sensitive Private Information from disclosure to third parties.

329. Defendant breached this duty by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

330. It was reasonably foreseeable that Defendant's failures to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members'

Private Information through its use of the Meta Pixels and other tracking technologies would result in unauthorized third parties, such as Meta, gaining access to such Private Information for no lawful purpose.

331. Defendant's duty of care to use reasonable measures to secure and safeguard Plaintiff's and Class Members' Private Information arose due to the special relationship that existed between Defendant and its patients, which is recognized by statute, regulations, and the common law.

332. In addition, Defendant had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of clients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

333. Defendant Wellstar's duty to use reasonable security measures under HIPAA required Defendant Wellstar to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare,

medical, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

334. In addition, Defendant Wellstar had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

335. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their Private Information.

336. Defendant's misconduct included the failure to (1) secure Plaintiff's and Class Members' Private Information; (2) comply with statutory duties to protect said Private Information from unauthorized disclosure, including pursuant to HIPAA and Section 5 of the FTC Act; (3) implement adequate website and event monitoring; (4) implement the systems, policies, and procedures necessary to prevent unauthorized disclosures resulting from the use of the Meta Pixels and other tracking technologies; and (5) prevent unauthorized access to Plaintiff's and Class Members' Private Information by sharing that information with Meta and other third parties. Defendant's failures and breaches of these duties constituted negligence per se.

337. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and Class members' Private Information, Plaintiff and the Class have suffered damages that include, without limitation, loss of the benefit of the bargain, increased infiltrations into their privacy through spam and targeted advertising they did not ask for, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

338. Defendant's wrongful actions and/or inactions and the resulting unauthorized disclosure of Plaintiff's and Class members' Private Information constituted (and continue to constitute) negligence at common law.

339. Plaintiff and Class Members are entitled to compensatory, nominal, and/or punitive damages, and Plaintiff and Class Members are entitled to recover those damages in an amount to be determined at trial.

340. Defendant Wellstar's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner. Therefore, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant Wellstar to (i) strengthen its data security systems and monitoring procedures; (ii) cease sharing Plaintiff's and Class Members' Private Information with Facebook and other third parties without Plaintiff's and Class

Members' express consent and (iii) submit to future annual audits of its security systems and monitoring procedures.

COUNT V

BREACH OF IMPLIED CONTRACT

(On behalf of Plaintiff & the Class)

341. Plaintiff repeats the allegations contained in the foregoing paragraphs preceding this Counts Section as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

342. When Plaintiff and Class Members provided their User data, such as PHI and PII, to Defendant Wellstar in exchange for services, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

343. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

344. Plaintiff and Class Members would not have entrusted Defendant Wellstar with their Private Information in the absence of an implied contract between them and Defendant Wellstar obligating Defendant not to disclose this Private Information without consent.

345. Defendant Wellstar breached these implied contracts by disclosing Plaintiff's and Class Members' Private Information to a third party, *i.e.*, Meta.

346. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiff and Class Members sustained damages as alleged herein. Plaintiff and Class Members would not have used Defendant's services, or would have paid substantially for these services, had they known their Private Information would be disclosed.

347. Plaintiff and Class Members are entitled to compensatory and consequential damages as a result of Defendant's breach of implied contract.

COUNT VI

BREACH OF EXPRESS CONTRACT
(On behalf of Plaintiff & the Class)

348. Plaintiff repeats the allegations contained in the foregoing paragraphs preceding this Counts Section as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

349. Plaintiff and Class Members allege they entered into valid and enforceable express contracts or were third-party beneficiaries of valid and enforceable express contracts with Defendant for the provision of medical and health care services.

350. Specifically, Plaintiff and Class Members entered into a valid and enforceable express contract with Defendants when Plaintiff and Class Members first received medical care from Defendant.

351. The valid and enforceable express contracts to provide medical and health care services that Plaintiff and Class Members entered into with Defendant include Defendant's promise to protect nonpublic, Private Information given to Defendant or that Defendant gathers on their own from disclosure.

352. Under these express contracts, Defendant and/or their affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members and (b) protect Plaintiff's and Class Members' PII/PHI: (i) provided to obtain such healthcare and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

353. Both the provision of medical services and the protection of Plaintiff and Class Members' Private Information were material aspects of these express contracts and exist independent of any duties under state or federal law, such as HIPAA.

354. The express contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiff and Class Members' Private Information—are formed and embodied in multiple documents, including (among other documents) Defendant's Privacy Notice.

355. At all relevant times, Defendant expressly represented in their Privacy Notice, among other things: (i) that Wellstar is "committed to keeping [Plaintiff's

and Class Members'] health information private"; (ii) that "uses and disclosures of [Plaintiff's and Class Members'] PHI not described in this Notice will be made only with [Plaintiff's and Class Members'] written authorization"; and (iii) that it may "not use and disclose [Plaintiff's or Class Members'] PHI for marketing purposes except in limited circumstances as authorized by law or unless [Plaintiff's or Class Members'] have given us written authorization."[81]

356. Defendant's express representations, including, but not limited to, express representations found in their Privacy Notice, formed and embodied an express contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

357. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiff and Class Members would

---

[81] https://www.wellstar.org/financial-policy-and-privacy-info/joint-notice-of-privacy-practices (last visited Apr. 12, 2023).

not have entered into these contracts with Defendant and/or their affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their Private Information would be safeguarded and protected.

358. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendant and/or their affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, both the provision of healthcare and medical services and the protection of their Private Information.

359. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

360. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when it disclosed that Private Information to Meta through the Meta Collection Tools, including the Meta Pixel on its Web Properties.

361. Defendant materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant Privacy Notice. Defendant did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by Defendant's sharing of that Private Information with Meta through the Meta Collection Tools, including the Meta Pixel on its Web

Properties. Specifically, Defendant did not comply with industry standards, or otherwise protect Plaintiff's and Class Members' Private Information, as set forth above.

362. The mass and systematic disclosure of Plaintiff's and Class Members' Private Information to third parties, including Meta, was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

363. As a result of Defendant's failure to fulfill the data privacy protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data privacy protection they paid for and the healthcare they received.

364. Had Defendant disclosed that its data privacy was inadequate or that it did not adhere to industry-standard privacy measures, Plaintiff, Class Members and any reasonable person would not have purchased healthcare from Defendant and/or their affiliated healthcare providers.

365. In addition, or in the alternative, Defendant breached the express contracts by breaching the implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a

contract's actual and/or express terms. In Georgia, a breach of contract claim may lie where the defendant acts in bad faith when exercising discretion over the performance of its duties under the contract.[82]

366. Here, Defendant acted in bad faith and/or with malicious motive in denying Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties and breached the implied covenant of good faith and fair dealing by presenting its healthcare services as private and secure, while secretly, systematically, and repeatedly disclosing Private Information to Meta through the Meta Collection Tools, failing to disclose to Plaintiff and Class Members that it disclosed Private Information to Meta through the Meta Collection Tools, and continuing to disclose Private Information to Meta through the Meta Collection Tools even after being called out in the media for its egregious acts.

367. As a direct and proximate result of the disclosure of Plaintiff's and Class Members' Private Information to Meta, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their Private Information, the loss of control of their Private Information, the imminent

[82] *See, e.g.*, *ULQ, LLC v. Meder*, 293 Ga. App. 176, 179, 666 S.E.2d 713, 717 (2008) ("where the manner of performance is left more or less to the discretion of one of the parties to the contract, he is bound to the exercise of good faith").

risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

368. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the disclosure of Plaintiff's and Class Members' Private Information to Meta.

COUNT VII
UNJUST ENRICHMENT
(On behalf of Plaintiff & the Class)

369. Plaintiff repeats the allegations contained in the foregoing paragraphs preceding this Counts Section as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

370. This count is pled in the alternative to Plaintiff's Breach of Implied Contract and Breach of Express Contract counts.

371. Defendant Wellstar benefits from Plaintiff and Class Members and unjustly retained those benefits at their expense.

372. Plaintiff and Class Members conferred a benefit upon Defendant Wellstar in the form of Private Information that Defendant collected from Plaintiff and Class Members, without authorization and proper compensation. Defendant consciously collected and used this information for its own gain, providing

Defendant with economic, intangible and other benefits, including substantial monetary compensation.

373. That is, in exchange for disclosing the PII of its patients, Defendant is compensated by Facebook in the form of enhanced advertising services and more cost-efficient marketing on Facebook. By utilizing the Meta Pixel, the cost of advertising and retargeting was reduced, thereby benefiting Defendant.

374. Defendant unjustly retained those benefits at the expense of Plaintiff and Class Members because Defendant's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members.

375. The benefits that Defendant Wellstar derived from Plaintiff and Class Members were not offered by Plaintiff and Class Member gratuitously and rightly belong to Plaintiff and Class Members. It would be inequitable under unjust enrichment principles in Georgia for Defendant to be permitted to retain any of the revenue or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

376. Defendant Wellstar should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

COUNT VIII

VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2511(1), *et seq*.
Unauthorized Interception, Use and Disclosure
(On Behalf of Plaintiff & the Class)

377. Plaintiff repeats the allegations contained in the foregoing paragraphs preceding this Counts Section as if fully set forth herein and brings this claim individually and on behalf of the Class.

378. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

379. The ECPA protects both the sending and receipt of communications.

380. The ECPA provides a private right of action to any person whose electronic communications are intercepted. 18 U.S.C. § 2520(a).

381. Wellstar intentionally intercepted electronic communications that Plaintiff and Class Members exchanged with Wellstar through the Meta Collection Tools installed on Wellstar's Web Properties.

382. The transmissions of data between Plaintiff and Class Members and Wellstar qualify as communications under the ECPA. 18 U.S.C. § 2510(12).

383. Wellstar contemporaneously intercepted and transmitted Plaintiff's and Class Members' communications to Meta.

384. The intercepted communications include:

a. the content of Plaintiff's and Class Members' registrations for the Patient Portal, including clicks on buttons to "Register" or "Signup" for portals;

b. the content Plaintiff's and Class Members' log in and log out of the Patient Portal, including clicks to "Sign-in," or "Log-in";

c. the content of communications that Plaintiff and Class Members exchanged inside the Patient Portal immediately before logging out of the portal, specifically including the act of paying medical bills;

d. the content of Plaintiff's and Class Members' communications relating to appointments with medical providers;

e. upon information and belief, the content of Plaintiff's and Class Members' communications relating to specific healthcare providers, conditions, treatments, diagnoses, prognoses, prescription drugs, symptoms, insurance and payment information; and

f. Full-string URLs that contain any information concerning the substance, purport, or meaning of patient communications with their health entities.

385. For example, Defendant's interception of the fact that a patient views a webpage like *"https://www.wellstar.org/medical-services/health-conditions-diseases/breast-cancer"* involves "content," because it communicates that patient's request for the information on that page.

386. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. the cookies Wellstar and Meta use to track Plaintiff's and Class Members' communications;

b. Plaintiff's and Class Members' browsers;

c. Plaintiff's and Class Members' computing devices;

d. Wellstar's web-servers or webpages where the Meta Collection Tools are present;

e. Meta's web-servers; and

f. the Meta Collection Tools source code Wellstar deploys on its Web Properties to acquire Plaintiff's and Class Members' communications.

387. Meta is not a party to Plaintiff's and Class Members' communications with Wellstar.

388. Wellstar transmits the content of Plaintiff's and Class Members' communications to Meta through the surreptitious redirection of those communications from Plaintiff's and Class Members' computing devices.

389. Plaintiff and Class Members did not consent to Meta's acquisition of their patient portal, appointment, and treatment communications with Wellstar.

390. Meta did not obtain legal authorization to obtain Plaintiff's and Class Members' communications with Wellstar relating to communications with their health entities.

391. Meta did not require Wellstar to obtain the lawful rights to share the content of Plaintiff's and Class Members' communications relating to patient portals, appointments and treatments.

392. Any purported consent that Meta received from Wellstar to obtain the content of Plaintiff's and Class Members' communications was not valid.

393. In disclosing the content of Plaintiff's and Class Members' communications relating to patient portals, treatments, conditions and appointments, Wellstar had a purpose that was tortious, criminal and designed to violate federal and state constitutional and statutory provisions and common law including:

a. the unauthorized disclosure of IIHI is tortuous in and of itself regardless of whether the means deployed to disclose the information violates the Wiretap Act or any subsequent purpose or use for the acquisition. Wellstar intentionally committed a tortious act by disclosing IIHI without authorization to do so.

b. the unauthorized acquisition of IIHI is a criminal violation of 42 U.S.C. § 1320d-6 regardless of any subsequent purpose or use of the IIHI. Wellstar intentionally violated 42 U.S.C. 1320d-6 by intentionally disclosing IIHI without authorization.

c. a violation of HIPAA, particularly 42 U.S.C. § 1320d-6, which is a criminal offensive punishable by fine or imprisonment with *increased penalties* where "the offense is committed with intent to sell, transfer or use IIHI for commercial advantage [or] personal gain." Wellstar intentionally violated the enhanced penalty provision of 42 U.S.C. § 1320d-6 by disclosing the IIHI

"with intent to sell transfer or use" it for "commercial advantage [or] personal gain."

d. a knowing intrusion upon Plaintiff's and Class Members' seclusion;

e. trespass upon Plaintiff's and Class Members' personal and private property via the placement of an _fbp cookie associated with Wellstar's Web Properties on Plaintiff's and Class Members' personal computing devices;

f. the requirements under O.C.G.A. § 31-33-2 and O.C.G.A. § 31-33-8 that healthcare providers maintain the confidentiality of patient health records; and

g. violation of the federal wire fraud statutes at 18 U.S.C. §§ 1343 (fraud by wire, radio, or television) and 1349 (attempt and conspiracy), which prohibit a person from "devising or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate … commerce, any writing, signs, signals, pictures, or sounds for purpose of executing such scheme or artifice."

394. The federal wire fraud statute, 18 U.S.C. § 1343, has four elements: (1) that the defendant voluntarily and intentionally devised a scheme to defraud another out of money or property; (2) that the defendant did so with the intent to defraud; (3) that it was reasonably foreseeable that interstate wire communications would be used and (4) that interstate wire communications were in fact used.

395. The attempt version of the wire fraud statute provides that "[a]ny person who attempts or conspires to commit any offense under this chapter shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy." 18 U.S.C. § 1349.

396. Wellstar's scheme or artifice to defraud in this action consists of:

a. the false and misleading statements and omissions in its privacy policies set forth above, including the statements and omissions recited in the breach of contract and negligence claims below;

b. the placement of the 'fbp' cookie on patient computing devices disguised as a first-party cookie of Wellstar's Web Properties rather than a third-party cookie from Meta.

397. Wellstar acted with the intent to defraud in that it willfully invaded and took Plaintiff's and Class Members' property:

a. property rights to the confidentiality of their IIHI and their right to determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes; and

b. property rights to determine who has access to their computing devices.

398. Wellstar acted with the intent to defraud in that it willfully invaded and took Plaintiff's and Class Members' property:

a. with knowledge that (1) Wellstar did not have the right to share such data without written authorization; (2)

courts had determined that a healthcare providers' use of the Meta Pixel gave rise to claims for invasion of privacy and violations of state criminal statutes; (3) a reasonable Facebook user would not understand that Meta was collecting their IIHI based on their activities on Wellstar's Web Properties; (4) "a reasonable Facebook user would be shocked to realize" the extent of Meta's collection of IIHI; (5) a Covered Incident had occurred which required a report to be made to the FTC pursuant to Meta's consent decrees with the FTC and (6) the subsequent use of health information for advertising was a further invasion of such property rights in making their own exclusive use of their IIHI for any purpose not related to the provision of their healthcare; and

b. with the intent to (1) acquire Plaintiff's and Class Members' IIHI without their authorization and without their healthcare providers or covered entities obtaining the right to share such information; (2) use Plaintiff's and Class Members' IIHI without their authorization; and (3) gain access to Plaintiff's and Class members' personal computing devices through the 'fbp' cookie disguised as a first-party cookie.

399. Any purported consent provided by Wellstar using the Meta Collection Tools had a purpose that was tortious, criminal, and in violation of state constitutional and statutory provisions because it constitutes:

a. knowing intrusion into a private matter that would be highly offensive to a reasonable person;

b. a violation of 42 U.S.C. § 1320d-6, which is a criminal offense punishable by fine or imprisonment and that includes increased penalties where "the offense is committed with intent to sell, transfer, or use

individually-identifiable health information for commercial advantage [or] personal gain."

c. trespass;

d. breach of fiduciary duty; and

e. a violation of various state health privacy and computer privacy statutes, including the CCPA and the CIPA.

400. Plaintiff and Class Members have suffered damages because of Wellstar's violations of the ECPA that include:

a. Wellstar eroded the essential, confidential nature of the provider-patient relationship;

b. Wellstar failed to provide Plaintiff and Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information;

c. Wellstar derived valuable benefits from using and sharing the contents of Plaintiff's and Class Members' communications on its Web Properties without their knowledge or informed consent, and without providing any compensation for the information it used or shared;

d. Wellstar's actions deprived Plaintiff and Class Members of the value of their IIHI;

e. Wellstar's actions diminished the value of Plaintiff's and Class Members' property rights in their IIHI; and

f. violating Plaintiff's and the Class Members' privacy rights by sharing their IIHI for commercial use.

401. For Wellstar's violations set forth above, Plaintiff and Class Members seek appropriate equitable or declaratory relief, including injunctive relief; actual damages and "any profits made by [Wellstar] as a result" of its violations or the appropriate statutory measure of damages; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred pursuant to 18 U.S.C § 2520.

402. Unless enjoined, Wellstar will continue to commit the violations of law alleged here.

403. Plaintiff wants to continue to communicate with their healthcare provider through online platforms but has no practical way of knowing if their communications are being intercepted and disclosed to Meta, and thus continues to be at risk of harm from Wellstar's conduct.

404. Pursuant to 18 U.S.C. § 2520, Plaintiff and Class Members seek monetary damages for the *greater of* (i) the sum of the actual damages suffered by Plaintiff and any revenue made by Wellstar as a result of the violation or (ii) statutory damages of whichever is greater of $100 a day for each violation or $10,000.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class Members, respectfully requests judgment in their favor and against Defendant and that the Court grant the following:

A. an Order certifying the Class and appointing Plaintiff and their Counsel to represent the Class;

B. equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;

C. injunctive relief requested by Plaintiff including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members;

D. an award of damages, including, but not limited to, actual, consequential, punitive, and nominal damages, as allowed by law in an amount to be determined;

E. an award of attorneys' fees, costs, and litigation expenses, as allowed by law, including, but not limited to, O.C.G.A. § 13-6-11, due to Defendant's bad faith in deceitfully and purposefully procuring Plaintiff's and Class Members' Private Information, payment, and other consideration with no intent to honor its promises to keep their Private Information confidential;

F. prejudgment interest on all amounts awarded; and

G. such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: April 23, 2024

Respectfully Submitted,

PEIFFER WOLF CARR KANE CONWAY & WISE, LLP

By: *<u>/s/ Andrew R. Tate</u>*
Andrew R. Tate
GA Bar # 518068
235 Peachtree St. NE, Suite 400
Atlanta, GA 30303
Ph: 404-282-4806
atate@peifferwolf.com

<u>/s/ Brandon M. Wise</u>
Brandon M. Wise
IL Bar # 6319580*
One US Bank Plaza, Suite 1950
St. Louis, MO 63101
Ph: (314) 833-4825
bwise@peifferwolf.com

ALMEIDA LAW GROUP LLC

<u>/s/ David S. Almeida</u>
David S. Almeida
NY Bar # 3056520*
Elena Belov
NY Bar # 4080891*
Britany Kabakov
IL Bar # 6336126*
849 W. Webster Avenue
Chicago, Illinois 60614
Ph: (312) 576-3024
david@almeidalawgroup.com

elena@almeidalawgroup.com
britany@almeidalawgroup.com

**pro hac vice to be sought*

Counsel for Plaintiff & the Proposed Class